VIF Brief | February 2021

THE CURIOUS CASE OF HUAWEI

Anurag Sharma

Vivekananda International Foundation

Published in 2021 by
Vivekananda International Foundation

3, San Martin Marg | Chanakyapuri | New Delhi - 110021

Tel: 011-24121764 | Fax: 011-66173415

E-mail: info@vifindia.org

Website: www.vifindia.org

Follow us on
Twitter | @vifindia

Facebook | /vifindia

Anurag Sharma is a Research Associate at Vivekananda International Foundation (VIF). He has completed MPhil in Politics and International Relations on 'International Security' at the Dublin City University in Ireland, in 2018. His thesis is titled as "The Islamic State Foreign Fighter Phenomenon and the Jihadi Threat to India". Anurag's main research interests are terrorism and the Internet, Cybersecurity, Countering Violent Extremism/Online (CVE), Radicalisation, Counter-terrorism and Foreign (Terrorist) Fighters. Prior to joining the Vivekananda International Foundation, Anurag was employed as a Research Assistant at Institute for Conflict Management. As International affiliations, he is a Junior Researcher at TSAS (The Canadian Network for Research on Terrorism, Security, And Society) in Canada; and an Affiliate Member with AVERT (Addressing Violent Extremism and Radicalisation to Terrorism) Research Network in Australia. Anurag Sharma has an MSc in Information Security and Computer Crime, major in Computer Forensic from University of Glamorgan (now University of South Wales) in United Kingdom and has an online certificate in 'Terrorism and Counterterrorism' from Leiden University in the Netherlands, and an online certificate in 'Understanding Terrorism and the Terrorist Threat' from the University of Maryland, the United States.

The Curious Case of Huawei

"Good surveillance is always dependent on the best available technology".

- H. Keith Melton (former US intelligence historian)[1]

China's journey from being an agrarian economy to one of the largest economies with a strong military and cyber capabilities is commendable. However, its military and cyber capabilities are built upon relentless efforts to steal critical military and technical information of other countries, mainly the United States (US).[2] Leading Chinese companies, including one of the telecom giants—Huawei Technologies Co. Ltd. (hereafter Huawei), are taking advantage of China's Belt and Road Initiative (BRI) projects to access the competitive neighbourhood nations. Huawei's 5G network may offer several benefits to any nation's essential infrastructure(s) such as transportation, technical capabilities, Fintech, and healthcare, among other sectors. These infrastructures are often considered critical to the nation and require the partnership of government and public-private entities to assess and further mitigate associated risks.

On 19 June 2020, the Australian Prime Minister (PM) Scott Morrison confirmed the multiple events of "sophisticated State-based cyber hack" and indirectly

signalled that China is behind the cyber-attacks on Australia's government, industry, political organisations, and other establishments. Adding to the strong suspicion of the Australian PM, thesecurity experts (based on anonymity) emphasised that the motive behind these attacks was China's restlessness after Australia had urged for an international inquiry to investigate the coronavirus pandemic's origins.[3]

Amid the concerns of China-led cyber-espionage, the United States (US), Australia and NATO (North Atlantic Treaty Organisation) nations are on guard and perceive China's Huawei's access into their respective technology market as a threat to the national security. The US and its allied nations' trade restrictions coupled with thecoronavirus pandemic may continue to impact Huawei's business worldwide negatively. This write-up attempts to analyse if China's Huawei is a boon to the evolving telecommunication technology or a digital espionage tool posing a threat to national security.

The Chinese Art of Deception & Emergence of Huawei

China's renowned "the Great Wall" is a gigantic historical artefact and a mysterious structure. The great wall gives an impression that the emperors built it to protect China from foreign invasions; however, as a massive symbol of the imperialism, the structure could have been a strategy to prove to and impress the public that the emperor has done something to protect the nation and therefore, has the mandate to rule. Further implementing the "Great Wall" theory in the cyber and information age, China's authoritarian regime decided to monitor and control the Internet traffic entering and leaving China. In 1998, the government had introduced the "Great Firewall of China" (GFC/GFWC) project administered by the Cyberspace Administration of China (CAC). The CAC is a state-owned Internet regulator, censor, oversight, and control agency.[4] The GFC is a combination of legal and technological actions to regulate the Internet domestically. As the purpose of the "Great Wall", the GFC was presented as a "digital firewall" to protect Chinese cyberspace from the invaders. On the contrary, the GFC imposes Internet censorship in the country and indirectly compels foreign companies to

adopt domestic regulations while doing business with Chinese entities.

As an emerging superpower in Asia, China has been applying the modus operandi of ancient Greeks (referring to theGreek mythology of the Trojan Horse) to invade other nations under the deceptive umbrella of development projects, technological assistance, and bilateral economic agreements. To compete with the United States (US) and establish the hegemony with technological advancement, China imitates the technology and project itself as an innovative nation. In October 2015, China had announced its plan of "Made in China (MIC) 2025" with the investment of USD 300 billion to become a high-tech powerhouse. According to the strategy, China promotes the manufacturing and supply of high-quality tech goods and services, such as robotics, Electric Vehicles (EV), Artificial Intelligence (AI), biotech, and aerospace.[5] The MIC 2025 was inspired by Germany's "Industry 4.0" plan of application of information technology to manufacturing of products and services. The focus on the innovation was inspired or "copied" from several likewise programmes already developed by the United States (US), Japan and the European Union (EU) in the 2000s information technology revolution.[6]

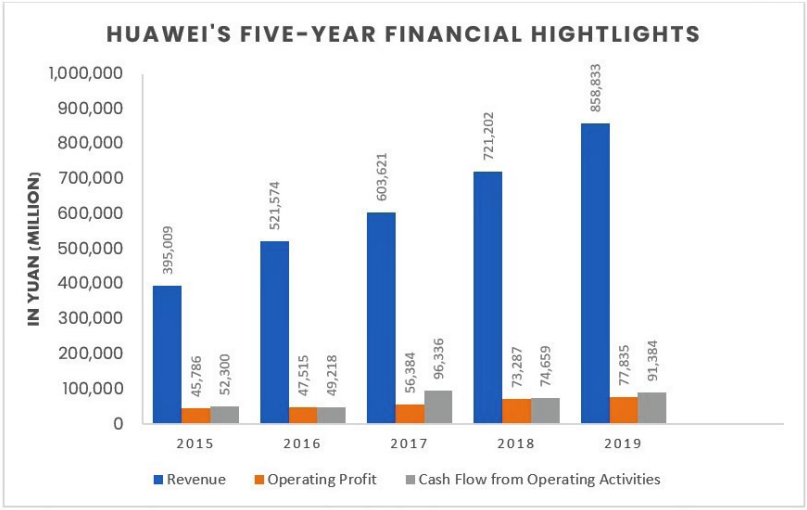
Brief Background of Huawei

China-based Huawei has emerged as one of the largest telecommunications equipment providers globally. Apart from the Information and Communication Technology (ICT) infrastructure, Huawei sells consumer devices such as laptops, wearables, sound devices, and smartphones. In the journey of over three decades, the company employs 194,000+ people, operating in more than 170 countries and regions and providing services to more than three billion people worldwide.[7] The telecommunication infrastructure, among various other functions, controls how the data traverse through the Internet. Huawei designs and manufactures the telecommunication infrastructure equipment such as antennas, network switches, gateways, routers, and bridges which plays a crucial role in the telecommunication infrastructure's operational capacity.

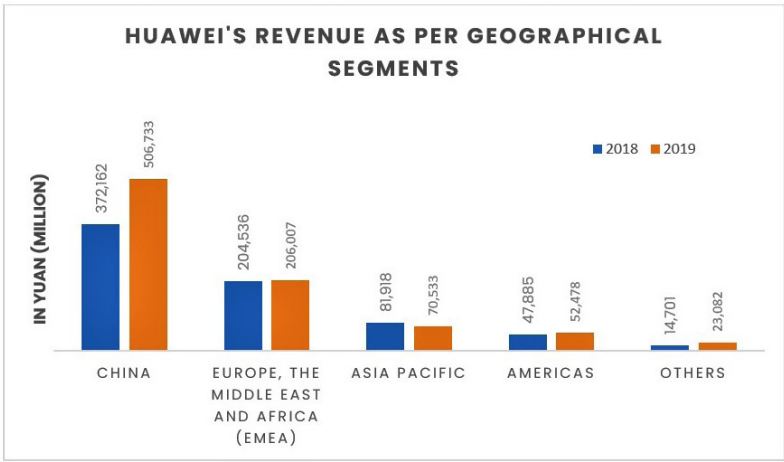
The company was founded in 1987 under Ren Zhengfei—a former Deputy Regimental Chief in China's People Liberation Army (PLA), with a mere

investment of Yuan 21,000 or approx. USD 3,000 (of today); and over time, it has emerged as one of the tech giants with the annual revenue of Yuan 8,58,833 million or USD 122,972 million in 2019.[8] In its journey of more than 30 years, Huawei has obtained 46 commercial 5G network contracts in 30 countries, with more than 100,000 5G base stations worldwide.[9] Despite allegations of espionage on behest of the Chinese government, Huawei and its subsidiaries continue to expand its business outside China. As per data estimates, most of the equipment used in 2G, 3G, and 4G networks in the United Kingdom and Europe, is produced by Huawei. The firm occupies 50 per cent of the market share of Vodafone UK's 2G, 3G and 4G network.[10] With the partial ban of Huawei in the UK telecom market, the rival 5G suppliers, such as Nokia, Ericsson, and Samsung got golden opportunity to step in and replace Huawei.

On the allegations that the Chinese government is using Huawei to spy on its rival nations, Ren Zhengfei countered the allegations by saying that "I support the Communist Party of China, but I will never do anything to harm any other nation. We would rather shut Huawei down than to damage the interests of our customers".[11]



Graph 1. Huawei's Five-Year Financial Highlights [Data Source: Huawei Annual Report 2019]



Graph 2. Huawei's Revenue break-up as per geographical segments for the years 2018 and 2019 [Data Source: Huawei Annual Report 2019]

Graph 1 and 2 highlights Huawei's revenue over the five-year, i.e. from 2015 to 2019. The significant rise of 19 per cent in revenue has been recorded from CYN 721,202 million (in 2018)/USD 106,201 million to CYN 858,833 million (in 2019)/USD 126,468 million. Despite US-China economic tensions, the revenue has shown progress in 2019. As an observation, Graph 1 and Graph 2 depict the increase in revenue by 09.59 per cent in the Americas region; but in the Asia-Pacific, Huawei's revenue declined by 13.9 per cent in 2018-2019.

Undoubtedly, the revenue of Huawei had a whopping increase in the domestic market—China, but as of trade restrictions, the relationship between Huawei and the allies of the US has been affected drastically. Due to coronavirus pandemic in 2020, Huawei's financial chart for the year would be different as compared to previous years. As a projection for 2020, Huawei's Rotating Chairman Eric Xu, in December 2019, has informed its employees in a New Year's message that the year 2020 would be challenging. The external milieu has become more complicated than before [referring to US-China trade tensions]. "In long-term, the US government shall continue to suppress and challenge the survival of Huawei", said Eric Xu.[12]

Reassessment of Relations with Huawei

Singing to the United States' (US) tunes, the United Kingdom (UK), and other European countries are reassessing their relations with Huawei. There was speculation among various news media if Germany would join the league to ban Huawei from its 5G rollout completely. Around 65 per cent of Deutsche Telekom's, 50 per cent of Vodafone's and Telefonica's telecommunications equipment are of Huawei.[13] Under Chancellor Angela Merkel's leadership, the German government holds the stance against security division to prevent a formal ban on Huawei.[14] The proposed regulation would tighten the scrutiny over international equipment vendor—Huawei in this case. According to the provisional draft proposed in Germany's IT Security Act2.0, the individual components would go through a technical test combined with the political assessment of the manufacturers' trustworthiness.[15]

As reported on 08 December 2020, the Finnish parliament (Eduskunta) passed the proposed bill (TPA 151/2020) to exclude Chinese companies—Huawei and ZTE from "tendering telecom bids in Finland, to restrict the use of their equipment, and to oblige companies and administration to eliminate all Chinese companies' 5G technology within the transition period".[16] In the ongoing storm of trade-war between two superpowers [the US and China], France has instructed its telecom operators that the licenses for Huawei's 5G equipment will not be renewed after its expiration. France's cybersecurity agency—ANSSI would allow telecom operators to use Huawei equipment but under the license of three to eight years.[17]

On 17 December 2018, the Czech Republic's National Office for Cyber and Information Security (NUKIB) has warned its intelligence-sharing allies over China's legal and political milieu, in which companies such as Huawei, exist and operate. The NUKIB's Director Dusan Navratil emphasised that Chinese laws required the companies-based in China to cooperate in its intelligence activities [including espionage], and therefore, with access to the critical systems may pose a significant threat.[18]

During the meeting between Russian President Vladimir V. Putin and Chinese President Xi Jinping at the International Economic Forum (IEF) held at St Petersburg in June 2019, Huawei has signed an agreement with Russian telecoms firm—MTS for development of 5G network in 2019-2020.[19] In the current milieu of geopolitics' dynamic scenario, China has applied *"enemy's enemy is a friend"* proverb. Citing Huawei and MTS's successful agreement in 2019, Huawei's founder Ren Zhengfei has said that post-US sanctions, Huawei transferred its investments from the US to Russia, increased Russian investment, expanded the Russian scientist team and made increments in the salaries of the Russian scientists.[20] On the other flip side of the same coin, Chinese investments in Russia and Huawei's cooperation in the development of Russia's 5G network gives Moscow and Beijing a sense of "win-win" situation. Russia lacks the alternative of Huawei but could offer a strong manufacturing base to China, with a robust local telecom market.

Security Concerns with Huawei and Its Subsidiaries

In its *Annual Report 2019,* Huawei claimed that no government agency or outside organisation holds shares in Huawei, but it is a private company—solely owned by its employees through an "Employee Shareholding Scheme" under the Union of Huawei Investment & Holdings Co. Ltd.[21] Contrary to the claims of Huawei management, on 03 January 2020, the US Federal Communications Commission (FCC) published a rule designating Huawei and ZTE Corporation (another China-based tech giant) having "strong ties with the Chinese government and military establishment—obligating under the Chinese laws to cooperate in compliance with the Chinese government to access their [Huawei and ZTE] systems.[22]

As Huawei is renowned for telecommunication products, the subsidiary company—Hi Silicon is known for manufacturing chips embedded in several IoT (Internet of Things)—based products, including CCTVs or other surveillance equipment. In February 2020, Vladislav Yarmak—a Russian Cyber Security Researcher, had revealed a backdoor mechanism discovered from Hangzhou Xiongmai Technology firmware—using HiSilicon chips to take control of several surveillance cameras, DVRs (Digital Video Recorder), NVRs (Network Video

Recorder), and other IoT devices.[23] The security blooper committed by Huawei's subsidiary—HiSilicon may not seem like a significant security threat, but it cannot be ignored either.

Undoubtedly, through such access, the Chinese government could carry out its cyber-espionage under the disguise of these companies and pose a threat to the security of communications networks and the supply chains. Supporting the Federal Communications Commission (FCC) rule, on 12 June 2020, the US Department of Defense (DoD) publicly released a list of 20 companies, including Huawei, labelling them as "Communist Chinese Military Companies", as a part of the 1999 National Defence Authorisation Act (NDAA). The list highlighted Chinese fusion of military-civil strategy of the People's Liberation Army (PLA) through certifying its access to advanced technologies acquired and developed by these Chinese companies, universities, and research programmes under the disguise of being civilian identities.[24]

In February 2020, in the Superseding Indictment (*Case 1:18-cr-00457-AMD*) filed against Huawei Technologies Co. Ltd and its five subsidiaries/partner companies, the United States government had identified Huawei's business relations in Iran, violating the laws and regulations, including sanction-related requirements. The US government's independent investigation had revealed Huawei's provisions of equipment and associated services, including surveillance technology, to the Iranian government, for monitoring, identifying and detaining the protestors during anti-government demonstrations in Tehran in 2009.[25] On 08 December 2020, *The Washington Post* published a news story based on Huawei's "Interoperability Report" discovered by the IPVM[26]; the report exposed the partnership between Huawei and Megvii (China-based facial recognition Software Company) providing a face recognition solution based on Huawei's video cloud solution. In 2018, Huawei and Megvii worked on artificial intelligence (AI) based camera systems that could scan faces in massive crowds and estimate individuals' age, sex, and ethnicity. The purpose of this facial recognition system is to send automated "Uyghur alarms" to Chinese authorities when the AI system identifies the Uyghur Muslims[27]—the oppressed minority group in Xinjiang, China.

The Five Eyes' Perception

Huawei's telecommunication equipment may raise concerns related to cyber-security in real, but it also highlights China's potential of being a contender to US' technological supremacy, mainly in cyber-security and networks. On Huawei's role and concerns of security, the Five Eyes intelligence alliance of Australia, Canada, New Zealand, the United Kingdom, and the United States, has placed restrictions on the use of Huawei's telecom equipment in their respective 5G networks. However, Canada is the only nation among Five Eyes who remains undecided on following the other four nations of intelligence alliance and freeze out the supplies from Huawei's for its 5G network. Australia and the US were first of the Five Eyes intelligence alliance to reject Huawei's equipment from 5G networks. Under Prime Minister Justin Trudeau, the Canadian government has not taken the security-related risks seriously and failed to ban Huawei from Canada's 5G network, which further puts Canada offside with its threat intelligence sharing partners, said Pierre Paul-Hus—a Canadian politician.[28]

In a year-long trade war initiated by the Trump administration, the US' allies and intelligence-sharing partners are in a state of dilemma in the conflict of two giant nations—the US and China. The United States intelligence agency—Central Intelligence Agency (CIA), in April 2019, has shared the intelligence information with its Five Eyes partners accusing Huawei of its links with the Chinese government and receiving funds from China's National Security Commission (NSC), the People's Liberation Army (PLA), and the third branch of the Chinese State intelligence network.[29]

Since the 1940s, the United Kingdom (UK) and the United States (US) have been sharing special relationship, from both World Wars to the modern era competition in the economic market. However, since 2018, the UK has been trying to balance the US' efforts to persuade its long-term ally [UK] to ban the 5G communication network and other telecommunication equipment from China's Huawei. In the early 2000s, UK's British Telecom (BT) had upgraded its network with the cheaper alternatives—of hundreds of millions of British pounds, offered

by Huawei. But the security concerns led the UK to form a special division to evaluate the Huawei's telecom equipment.

In November 2010, under the set of agreements between the Huawei Technologies (UK) Co. Ltd. under parent company—Huawei Technologies based in China, and Her Majesty's Government (HMG), a facility—Huawei Cyber Security Evaluation Centre (HCSEC) was established in Banbury in Oxfordshire; England to assess any perceived risks arises due to the involvement of Huawei in the UK's Critical National Infrastructure (CNI).[30] Addressing the Munich Security Conference in February 2019, UK's then-MI6 chief—Alex Younger said that Huawei's security risks are manageable; therefore, despite complexities around Huawei being a 5G technology supplier, an outright ban might not be necessary.[31] In the oversight report by the HCSEC published in September 2020, the investigators have revealed several vulnerabilities, mainly software design failure related, which could easily allow the hostile actors (Chinese government in this case due to Huawei) to carry out a cyber-attack.[32]

The UK's National Cyber Security Centre (NCSC)—a wing of the Government Communications Headquarters (GCHQ) has advised that there are significant concerns about vulnerability management in Huawei's equipment. Huawei's Software component management is defective, which further leads to higher vulnerability and significant risk of unsupportable software.[33] The US sanctions imposed on Huawei have resulted in a U-turn made by the UK government. The UK Prime Minister (PM)—Boris Johnson has banned the purchase of any Huawei telecommunication or related equipment from the end of 2020 and altogether remove Huawei's involvement in the UK's 5G network from the year 2027.[34] In August 2018, Huawei Australia tweeted that "We have been informed by the government [Australian] that Huawei & ZTE have been restricted from providing 5G technology to Australia".[35] The UK and Australia have sided with the US' campaign to take-out Huawei products; however, New Zealand and Canada are yet to decide on the complete barring of Huawei and may come up with comprehensive policies to deal with the threat posed by Huawei's equipment.

In November 2018, New Zealand government at the behest of its intelligence agency had rejected the bid request from its telecommunications service provider—Spark New Zealand Ltd, to use Huawei's 5G equipment, citing the concerns related to national security. However, Huawei has a large share in New Zealand's 4G network. Referring to the technical differences between 4G& 5G network and risks associated with the deployment of Huawei, New Zealand's Intelligence Services Minister—Andrew Little has said that in Huawei's 5G technology, every component and each part of a network can be accessed.[36] The unauthorised access will raise national security concerns over the deployment of Huawei's 5G network equipment in Critical National Infrastructure (CNI). Unlike the other four member nations of the Five-Eye intelligence alliance, New Zealand—with substantial dependence on China's goods and markets, may not have the capacity to bear the economic shocks emerged from the barring of Huawei telecommunications equipment in its telecom sector.

Indian Perspective on Huawei

India's ban on 118 Chinese apps, including PUBG and TikTok, was appreciated and followed by the US with banning TikTok application. In India, Huawei arrived not only through telecom equipment, but also by introducing consumer-end products and services such as smartphones, tablets, smart-watches, and sound/music accessories. During coronavirus *aka* Covid-19 pandemic and border tensions at the Line of Actual Control (LAC) with China, the Indian government has marked first significant economic move against China by suggesting telecom operators, including the Bharat Sanchar Nigam Limited (BSNL), and Mahanagar Telephone Nigam Limited (MTNL) to avoid using telecommunication equipment manufactured by Chinese companies such as Huawei, ZTE Corporation, and encouraged domestic telecom equipment makers to meet such requirements.[37] Unlike the US and UK, India has been ambiguous about imposing a complete or partial ban on Huawei considering the risks to national security and international pressure built-up by the US and its allies.

The Telecom Service Providers (TSPs) have been instructed to procure networking and telecommunication equipment under the existing general financial rules, further imposing restrictions on vendors from neighbouring countries sharing a land border with India. The Department of Telecommunications (DoT) had not issued any specific order; but has amended the Rule 144 of the General Financial Rules 2017—"*Fundamental Principles of public* buying" with the insertion of sub-rule (xi) by the Department of Expenditure which states that-

> *"Notwithstanding anything contained in these Rules, Department of Expenditure may, by order in writing, impose restrictions, including prior registration and/or screening, on procurement from bidders from a country or countries, or a class of countries, on the grounds of defence of India, or matters directly or indirectly related thereto including national security; no procurement shall be made in violation of such restrictions".*[38]

The ban on Huawei has put a question mark on the well-being of Indian telecom sector in the absence of capacities in the indigenous manufacturing of the telecommunication equipment; the sector is heavily dependent on both—Huawei and ZTE for their economic competitiveness compared to other vendors. Having two of India's largest telecom companies—Bharti Airtel and Vodafone-Idea as its clients, Huawei and ZTE hold around 55 per cent share of the Indian wireless telecom market.[39] Apart from the private telecommunication firms, the 3G network of the BSNL was built upon ZTE where it holds 40 per cent share in the total network.[40] The replacement of China-based telecommunication equipment with the "Made in India" equipment would not be an impossible task but achievable at a higher cost. According to figures of June 2020, the Indian telecom equipment market is worth INR 12000 crore in which China-made equipment share is around 25 per cent. Proscribing Chinese vendors may attract European vendors to supply the requirement; however, an increase of 15-20 per cent in their procurement cost will be hefty for the Indian telecom operators.[41]

Telecom Service Providers (TSPs)	Status with Telecom Equipment Deployment
Reliance Jio Infocom Limited (RJIL)	It has not deployed any telecom equipment deployment from Huawei and ZTE in its network to provide telecom services as per its Unified License (UL).
Vodafone Idea Limited (VIL)	Multi-vendors for equipment for different purposes in its network and has always compliant to security-related requirements placed upon by the DoT.
Bharti Airtel Limited (BAL)	It has multi-vendors partners, including Indian, American, European, and Chinese, to build a robust and secure network for its networks.
Bharat Sanchar Nagar Limited (BSNL)	Has 44.4 per cent of its mobile network equipment from ZTE, and 09 per cent from Huawei.[42]
Mahanagar Telephone Nigam Limited (MTNL)	Has 10 per cent of its mobile network equipment from Chinese manufacturers.[43]

Table 1. Information given by the DoT received from respective TSPs regarding deployment of telecom equipment from vendors [Source: DoT-Rajya Sabha][44]

In such a scenario, if restrictions on the use of Huawei manufactured telecommunications equipment in the Indian telecom market are pulled-off, India must acquire the source code of the telecom equipment [hardware/software] from the vendor, to ensure the zero-gap in security-related concerns further.

On 17 September 2020, the Minister of State for Communications, Education and Electronics & Information Technology [MoSCEE&IT]—Sanjay Dhotre had informed the Rajya Sabha [Upper House of the Parliament] that the security testing framework was mandatory under the Indian Telegraph (Amendment) Rules. Furthermore, under the framework of Mandatory Testing and Certification of Telecom Equipment [MTCTE], the National Centre for Communication Security [NCCS] has been formed with the responsibility to conduct tests of telecom products comprising of hardware and software.[45] Despite allowing Huawei to participate in 5G network trials in December 2019, the Indian government had told BSNL and MTNL not to use the Chinese equipment in 4G network upgrade,

and both State-run telecom providers [BSNL and MTNL] cancelled the tenders. Emphasising the "Make in India", new tenders will be floated with objectives of developing in-house technology.[46]

Road Ahead—"Vocal For Local"

Apart from Nokia and Ericsson, Huawei has become one of the foremost companies in 5G network research and development. On various allegations, Huawei has maintained that the company is owned by its employees and not by the Chinese government. On the contrary, the US has been arguing that Huawei's equipment may use malicious programmes as "backdoor" to do espionage on behest of the Chinese government. China's National Intelligence Law (NIL) 2017 (2018 Amendment) aimed at strengthening the legality to security and intelligence activities. The law required Chinese nationals, foreign citizens (based in China), and organisations (Headquartered in China) to cooperate with the Chinese government. The Article 7 of the National Intelligence Law 2017, states that "an organisation or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows."[47]

Supporting the US' argument, Jerome Cohen—a professor at the New York University, US, has said that "there is no way Huawei could resist any order from the Chinese government or the Chinese Communist Party and would have to respond with requested data and perform whatever other surveillance activities are required."[48] Amid ongoing suspicion on Huawei's technology, on 10 September 2020, the company has announced that HarmonyOS 2.0—Huawei's developed Operating System (OS) for smartphones will be available in 2021.[49] On the "backdoor" allegations in HarmonyOS, Huawei claimed that the Operating System's source code would be completely Open-Source, unlike Microsoft Inc. and Apple Inc., to examine any vulnerability in the Operating System.

For India, skilful engineers are plenty, but there is a need for the capacity building to locally manufacture 5G network equipment. With ample support from the Indian government, the phenomenon of "Vocal for Local" shall boost local

manufacturers' morale to provide Huawei's alternative over the period. With the vision to promote interoperability and innovation of the 5G ecosystem in India, the Department of Telecommunication (DoT) had approved the funding of ₹224.01 crores for a collaborative project to set up 'indigenous 5G Test Beds' in India by 01 April 2021, involving eight institutes—the Centre of Excellence in Wireless Technology (CEWT), IITs (Indian Institute of Technology—Delhi, Bombay, Hyderabad, Madras and Kanpur), IISc (Indian Institute of Science, Bangalore), and Society for Applied Microwave Electronics Engineering & Research (SAMEER).[50] In April 2020, Bharti Airtel had strengthened its 4G network and looked forward to developing 5G network by deploying 300,000 radio units pan India by 2022, under a multi-year deal worth USD 1 billion (approx. ₹7,636 crores) with Finnish tech giant Nokia.[51]

In June 2020, India's telecommunications giant—Reliance Jio had filed a request with the Department of Telecom (DoT) for an approval to commence 5G network testing in its labs.[52] In the following month (July 2020), in his address to the 43rd Reliance Annual General Meeting (AGM), Mukesh D Ambani (Chairman and MD of Reliance Industries) announced that "Jio has created a 5G solution from scratch, using 100 per cent homegrown technologies and solutions".[53] Many technical experts questioned and raised doubts regarding Reliance Jio's vision to bring indigenous 5G solution for India keeping pace with time and replacing China's Huawei. The vision would place India in a league of nations that offer the fastest connectivity to the users.

On 20 October 2020, Reliance Jio announced its partnership with US-based Qualcomm Incorporated, to develop an open and interoperable interface-based 5G solutions to achieve India's vision of 5G—based on indigenous technologies.[54] "Jio has indigenously developed a 5G RAN (Radio Access Network) product—already tested by a Tier-1 carrier in the US", said Mathew Oommen—President of Reliance Jio Infocomm.[55] Through its embraced digital and technological capabilities, Reliance Jio has emerged as one of the stable corporations in India's digital revolution. On successful tests, Reliance Jio is expected to be the first telecom carrier in the world to carry out the development of its 5G technology

without any partnership with other network providers such as Nokia, Ericsson, and Huawei.

Likewise, Five-Eyes intelligence alliance, a formation of "D-10" alliance—comprising G-7 nations plus India, Japan and South Korea, is highly likely to join the US-led campaign against China. Proposed by the United Kingdom (UK), the D-10 alliance would encourage more 5G technology and equipment providers from democratic regimes to marginalise China's Huawei alleviating any security concerns. Leveraging the golden opportunity, India must work on its existing technical capabilities and develop them to manufacture indigenous equipment required for telecom and communications-related sector. As a collaborative effort by various stakeholders, the Government of India and the Indian telecommunication industries should develop and strengthen the manufacturing capabilities in the sector at the "Next Generation" telecommunication facilities.[56] The Preferential Market Access (PMA) to indigenous manufactured telecommunication equipment—consistent with our commitments to the World Trade Organisation (WTO), was one of the objectives of the National Telecom Policy (NTP) 2012; therefore it should be carefully followed to encourage the local manufacturers to make India a "telecom equipment manufacturing hub". Progressing towards realising the vision of indigenous market of telecom equipment manufacturing, on 11 November 2020, the Indian government had approved ₹12,195 crores for the telecom equipment manufacturing under the Production-Linked Incentive (PLI) scheme supporting the manufacturing firms to export from India.[57] The risk comparison between India and other countries on the deployment of Huawei telecom equipment would be different. Given China's misdeeds against India on every front—political, military, diplomacy, and terrorism; China can exploit Huawei's network to target and attack India's Critical National Infrastructure (CNI). In ongoing geopolitical scenario and conceivable cyber-threats from China, mainly through Huawei, India cannot depend on manufacturing telecommunications equipment by other nations, certainly not on China.

Endnotes

1. Melton, Keith H. 2021. "High-tech surveillance and an eye in the sky", Spycraft (Documentary).

2. Singh, Bhopinder. "Chinese art of deceit", The Pioneer, 29 June 2020, Available from: https://www.dailypioneer.com/2020/columnists/chinese-art-of-deceit.html

3. Shears, Richard. "Australia's Prime Minister Scott Morrison urges UK to stay alert after his country was 'hit by huge China cyber hack' on businesses, schools and hospitals", Daily Mail UK, 19 June 2020, Available from: https://www.dailymail.co.uk/news/article-8441271/Australias-Prime-Minister-urges-UK-stay-alert-country-hit-huge-China-cyber-hack.html

4. Cheung, Jennifer. "China's great firewall just got taller", Open Democracy, 14 July 2015, Available from: https://www.opendemocracy.net/en/digitaliberties/chinas-great-firewall-just-got-taller/

5. Fang, Jason and Michael Walsh. "Made in China 2025: Beijing's manufacturing blueprint and why the world is concerned", ABC News, 29 April 2018, Available from: https://www.abc.net.au/news/2018-04-29/why-is-made-in-china-2025-making-people-angry/9702374

6. Kennedy Scott. "Made in China 2025", Center for Strategic & International Studies, 01 June 2015, Available from: https://www.csis.org/analysis/made-china-2025

7. "Our Company", Huawei, Available from: https://www.huawei.com/en/corporate-information

8. "2019 Annual Report", Huawei Investment & Holding Co. Ltd, Available from: https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report_2019_en.pdf?la=en

9. "Huawei obtains 46 commercial 5G contracts in 30 countries", Xinhua, 06 June 2019, Available from: http://www.xinhuanet.com/english/2019-06/06/c_138122365.htm

10. Fenn, Alec. "How Huawei's European growth started in the UK", CGTN, 15 July 2020, Available from: https://newseu.cgtn.com/news/2020-07-15/How-Huawei-s-European-growth-started-in-the-UK-S9uyuAsAiQ/index.html

11. Bowler, Tim. "Ren Zhengfei: Huawei's reclusive founder", BBC News, 18 February 2019, Available from: https://www.bbc.com/news/business-47279262

12. Goh, Brenda. "Huawei's 2019 revenue to jump 18%, forecasts 'difficult' 2020", Reuters, 31 December 2019, Available from: https://uk.reuters.com/article/us-huawei-tech-results/huaweis-2019-revenue-to-jump-18-forecasts-difficult-2020-idUKKBN1YY1JL

13. "Germany and Brazil looking to allow Huawei participate in their respective 5G projects", ET News—Korea IT News, 03 December 2020, Available from: https://english.etnews.com/20201203200002

14. Donahue, Patrick. "Merkel Resists Full Ban on Huawei, Making Germany an Outlier", Bloomberg, 22 September 2020, Available from: https://www.bloomberg.com/news/articles/2020-09-22/merkel-resists-full-ban-on-huawei-making-germany-an-outlier

15. Hoppe, To. and Moritz Koch. "High hurdles for Huawei—the procedure is equivalent to an exclusion", Handelsblatt, 29 September 2020, Available from: https://www.handelsblatt.com/politik/international/5g-mobilfunknetz-hohe-huerden-fuer-huawei-das-verfahren-kommt-einem-ausschluss-gleich/26229670.html?ticket=ST-8281111-ETSFgFUeMem2oJptSc9P-ap2 [translated by Google].

16. "Finnish parliament passes law banning Huawei, ZTE from supplying 5G equipment", Telecompaper, 08 December 2020, Available from: https://www.telecompaper.com/news/finnish-parliament-passes-law-banning-huawei-zte-from-supplying-5g-equipment--1364811 ; EU Reporter Correspondent. "Finnish Parliament considers banning Huawei and ZTE from supplying 5G equipment", EUReporter, 08 December 2020, Available from: https://www.eureporter.co/frontpage/2020/12/08/finnish-parliament-passes-law-banning-huawei-and-zte-from-supplying-5g-equipment/?utm_source=rss&utm_medium=rss&utm_campaign=finnish-parliament-passes-law-banning-huawei-and-zte-from-supplying-5g-equipment ; "Finnish Parliament considers banning Huawei and ZTE from supplying 5G equipment", News TL, 08 December 2020, Available from: https://news.tl/finnish-parliament-passes-law-banning-huawei-and-zte-from-supplying-5g-equipment-43480.html

17. Reuters. "France imposes de facto ban on Huawei 5G equipment, says report", Business Standard, 23 July 2020, Available from: https://www.business-standard.com/article/international/france-imposes-de-facto-ban-on-huawei-5g-equipment-says-report-120072300043_1.html

18. "Huawei and ZTE software and hardware are a security threat", NUKIB, 17 December 2018, Available from: https://nukib.cz/cs/infoservis/aktuality/1303-software-i-hardware-spolecnosti-huawei-a-zte-je-bezpecnostni-hrozbou/

19. Agencies. "China's Huawei signs deal to develop 5G network in Russia", The Guardian, 06 June 2019, Available from: https://www.theguardian.com/technology/2019/jun/06/chinas-huawei-signs-deal-to-develop-5g-network-in-russia

20. Chen, Celia. "Huawei has increased investment in Russia because of US sanctions, founder Ren Zhengfei says", South China Morning Post, 31 August 2020, Available from: https://www.scmp.com/tech/gear/article/3099528/huawei-has-increased-investment-russia-because-us-sanctions-founder-ren

21. Bowler, Tim. "Ren Zhengfei: Huawei's reclusive founder", BBC News, 18 February 2019, Available from: https://www.bbc.com/news/business-47279262

22. United States. "Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs; Huawei Designation; ZTE Designation", Federal Communications Commission, 03 January 2020, Available from:https://www.federalregister.gov/documents/2020/01/03/2019-27610/protecting-against-national-security-threats-to-the-communications-supply-chain-through-fcc-programs ; Federal Register :: Protecting Against National Security https://www.federalregister.gov/documents/2020/01/03/2019-27610/protecting-against-national-security-threats-to-the-communications-supply-chain-through-fcc-programs

23. Adrian Potoroaca. "Researcher says millions of IoT and surveillance devices that use HiSilicon chips have a trivial backdoor", Techspot, 07 February 2020, Available from: https://www.techspot.com/news/83909-researcher-millions-iot-surveillance-devices-use-hisilicon-chips.html

24. United States. "DOD releases list of additional companies in accordance with section 1237 of FY99 NDAA", Department of Defense, 28 August 2020, Available from: https://www.defense.gov/Newsroom/Releases/Release/Article/2328894/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/

25. United States of America Vs Huawei Technologies Co. Ltd. 2020. "Case 1:18-cr-00457-AMD", The Department of Justice, Available from: https://www.justice.gov/opa/press-release/file/1248961/download

26. IPVM is a team of 20 with extensive experience working for security integrators, organizations, and manufacturers as well as graduates from Columbia, Dartmouth, Harvard, Lehigh, Northwestern, NYU, RIT, West Point, UPenn, and Yale.

27. Harwell, Drew and Eva Dou. "Huawei tested AI software that could recognize Uighur minorities and alert police, report says", The Washington Post, 08 December

2020, Available from: https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says/

28. Fife, Robert, Alexandra Posadzki, Paul Waldie and Adrian Morrow. "Canada is now the only Five Eyes member to not ban or restrict use of Huawei 5G equipment", The Globe and Mail, 15 July 2020, Available from: https://www.theglobeandmail.com/politics/article-canada-now-only-member-of-five-eyes-alliance-to-have-not-banned-huawei/#:~:text=Australia%20and%20the%20United%20States,Washington%20for%20the%20U.K.%20rollback

29. Fisher, Lucy. "CIA warning over Huawei", The Sunday Times, 20 April 2019, Available from: https://www.thetimes.co.uk/edition/news/cia-warning-over-huawei-rz6xc8kzk

30. The United Kingdom. "Annual Report-Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board", National Cyber Security Centre, 2019, Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf

31. Mason, Rowena. "UK security chiefs: Huawei risk in 5G can be contained", The Guardian, 17 February 2019, Available from: https://www.theguardian.com/technology/2019/feb/17/uk-security-chiefs-huawei-risk-in-5g-can-be-contained

32. Martin, Alexander. "GCHQ discovered 'nationally significant' vulnerability in Huawei equipment", Sky News, 01 October 2020, Available from: https://news.sky.com/story/gchq-discovered-nationally-significant-vulnerability-in-huawei-equipment-12086688

33. The United Kingdom. "Annual Report-Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board", National Cyber Security Centre, 2020, Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923309/Huawei_Cyber_Security_Evaluation_Centre__HCSEC__Oversight_Board-_annual_report_2020.pdf

34. Heffer, Greg. "Huawei blocked: Tech must be stripped from UK's 5G network by 2027", Sky News, 15 July 2020, Available from: https://news.sky.com/story/huawei-blocked-tech-must-be-stripped-from-uks-5g-network-by-2027-12028177

35. Huawei Australia (@HuaweiOZ). 2018. "Huawei Australia Post". Twitter. 23 August 2018. 05:06 AM. Available from: https://twitter.com/HuaweiOZ/status/1032411216184930304

36. Greenfield, Charlotte. "New Zealand rejects Huawei's first 5G bid citing national security risk", Reuters, 28 November 2018, Available from: https://www.reuters.com/article/us-spark-nz-huawei-tech/new-zealand-rejects-huaweis-first-5g-bid-citing-national-security-risk-idUSKCN1NX08U

37. Mankotia, Anandita Singh. "Govt may bar Airtel, Vodafone Idea from using gear from Huawei, ZTE", The Economic Times, 18 June 2020, Available from: https://telecom.economictimes.indiatimes.com/news/big-blow-for-zte-huawei-india-to-bar-bsnl-from-sourcing-chinese-gear-may-also-bar-pvt-telcos/76431279

38. Government of India-Ministry of Communications. "Share of Huawei and ZTE in Telecom Market", Rajya Sabha, Unstarred Question no. 483, 17 September 2020, Available from: https://pqars.nic.in/annex/252/AU483.pdf ; "GFR: Insertion of Rule 144 (xi) in the General Financial Rules, 2017 – FINMIN O.M 23rd July, 2020", Staff News, 25 July 2020, Available from: https://www.staffnews.in/2020/07/gfr-insertion-of-rule-144-xi-in-the-general-financial-rules-2017-finmin-o-m-23rd-july-2020.html

39. Punit, Itika Sharma. "India's richest man is borrowing from the big tech playbook", Quartz India, 24 August 2020, Available from: https://qz.com/india/1893321/reliances-mukesh-ambani-is-on-a-spending-spree/

40. Rathee, Kiran. "Ban on equipment from Huawei, ZTE to cost Airtel, Voda-Idea, BSNL dear amid India-China faceoff", The Financial Express, 23 July 2020, Available from: https://www.financialexpress.com/industry/ban-on-chinese-vendors-to-cost-domestic-telecom-companies-dear-huawei-zte-boycott-china-bsnl-4g-bharti-airtel/1999946/

41. Ibid.

42. ENS Economic Bureau. "Over 50% equipment in BSNL mobile networks Chinese: Govt", The Indian Express, 18 September 2020, Available from: https://indianexpress.com/article/business/over-50-equipment-in-bsnl-mobile-networks-chinese-govt-6600371/

43. Ibid.

44. Government of India-Ministry of Communications. "Share of Huawei and ZTE in Telecom Market", Rajya Sabha, Unstarred Question no. 483, 17 September 2020, Available from: https://pqars.nic.in/annex/252/AU483.pdf

45. Ibid.; PTI. "DoT notifies additional telecom equipment for mandatory testing, certification", Telengana Today, 25 June 2020, Available from: https://telanganatoday.com/dot-notifies-additional-telecom-equipment-for-mandatory-testing-certification

46. "BSNL & MTNL Cancel 4G Tenders to Exclude Chinese Telecom Giants Huawei, ZTE After Govt Nudge", News 18, 01 July 2020, Available from: https://www.news18.com/news/business/bsnl-cancels-4g-tender-worth-rs-8000-crore-after-govt-says-no-to-use-of-chinese-telecom-gear-2696251.html

47. The People's Republic of China. "National Intelligence Law of the People's Republic of China (2018 Amendment)", 2018, Available from: https://en.pkulaw.cn/display.aspx?cgid=313975&lib=law ; Vahia, Shivam. "India's 5G dilemma: Hi Huawei or Bye Huawei?", CNBC TV18, 24 February 2020, Available from: https://www.cnbctv18.com/telecom/indias-5g-dilemma-hi-huawei-or-bye-huawei-5359391.htm

48. Kharpal, Arjun. "Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice", CNBC, 04 March 2019, Available from: https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html

49. Zhe, Gong. "Huawei's HarmonyOS 2.0 coming to smartphones in 2021", CGTN, 10 September 2020, Available from: https://news.cgtn.com/news/2020-09-10/Huawei-s-HarmonyOS-2-0-coming-to-smartphones-in-2021-TFLqH0vMeQ/index.html

50. Government of India-Ministry of Communications. "Network & Technologies", Department of Telecommunications, Available from: https://dot.gov.in/networks-technologies-cell

51. IANS. "Airtel signs ₹7,636 crore deal with Nokia to enhance 4G network, lay foundation for 5G network", Business Insider, 28 April 2020, Available from: https://www.businessinsider.in/business/telecom/news/airtel-signs-7636-crore-deal-with-nokia-to-enhance-4g-network-lay-foundation-for-5g-network/articleshow/75423000.cms

52. Jain, Rounak. "Even before the India-China clash, Asia's richest man Mukesh Ambani was working on replacing Huawei", Business Insider, 19 June 2020, Available from: https://www.businessinsider.in/business/telecom/news/even-before-the-india-china-clash-asias-richest-man-mukesh-ambani-was-working-on-replacing-huawei/articleshow/76460868.cms

53. Tech Desk. "Reliance Jio 'Made in India' 5G solution announced RIL AGM 2020: Details inside", The Indian Express, 16 July 2020, Available from: https://indianexpress.com/article/technology/tech-news-technology/reliance-jio-to-launch-made-in-india-5g-network-mukesh-ambani-6506961/

54. "Reliance Jio-Qualcomm 5G network deal: what does this mean for India?", Moneycontrol, 21 October 2020, Available from: https://www.moneycontrol.com/news/technology/reliance-jio-qualcomm-5g-network-deal-what-does-this-mean-for-india-5991271.html

55. PTI. "Jio platforms, Qualcomm successfully test 5G solutions, clock over 1 Gbps speed in trials", Yahoo Finance, 20 October 2020, Available from: https://in.finance.yahoo.com/news/jio-platforms-qualcomm-successfully-test-170033138.html

56. Excerpt from author's conversation with Dr Gulshan Rai, former National Cyber Security Coordinator (NCSC)—Government of India. Dated: 04 November 2020.

57. Guha, Ishita. "PLI for telecom sector to encourage Indian, global firms: Ravi Shankar Prasad", Mint, 11 November 2020, Available from: https://www.livemint.com/industry/telecom/pli-for-telecom-sector-to-encourage-indian-global-firms-ravi-shankar-prasad-11605108990257.html

About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non-partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organisation to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelise fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its inception, VIF has pursued quality research and scholarship and made efforts to highlight issues in governance, and strengthen national security. This is being actualised through numerous activities like seminars, round tables, interactive dialogues, Vimarsh (public discourse), conferences and briefings. The publications of VIF form lasting deliverables of VIF's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

VIVEKANANDA INTERNATIONAL FOUNDATION
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Phone: +91-11-24121764, 24106698
Email: info@vifindia.org,
Website: https://www.vifindia.org
Follow us on twitter@vifindia