Vivekananda International Foundation

5G, Huawei and India

Maj Gen PK Mallick, VSM (Retd)

VIF Brief - July 2019

Published in June 2019 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

About the Author

One of the foremost experts on electronics and communication, **Maj Gen PK Mallick**, VSM (Retd) is a graduate of Defence Services Staff College and M Tech from IIT, Kharagpur. He has wide experience in command, staff and instructional appointments in Indian Army. He has also been a Senior Directing Staff (SDS) at National Defence College, New Delhi. Presently, he is a Consultant with the Vivekananda International Foundation, New Delhi.

Introduction

The ability to create and use new technologies is the source of economic strength and military security. Technology and the capacity to create new technologies are the basis of information age power. 5G as the cornerstone of a new digital environment is the focal point for the new competition.

China's success in creating globally competitive tele-communications firms has led the Chinese government's desire to seize leadership in next generation Information Technology (IT). China is the world's largest manufacturer of Internet of Things (IoT) devices. The rapid increase in these largely unsecure IoT devices is creating numerous points of vulnerability to intelligence intrusion, cyber attacks, industrial control or censorship. Huawei's lead in 5G based technology surprised experts and competitors leaving old stalwarts like Nokia, Siemens and Ericsson years behind. US firms and the US government rely on global supply chains that in many cases are dominated by China. US and Chinese companies are engaged in a fierce competition to secure first mover advantage and benefit from the trillions in economic benefits 5G and subsequent technologies are expected to create. IoT devices collect enormous amounts of user information; when aggregated and combined with greater computing power and massive amounts of publicly available information, these data can reveal information the user did not intend to share.

Alarmed by the rapid progress of Huawei the US government has launched a concerted campaign both domestically and internationally to block Huawei from building Next-Generation (5G) wireless networks. The US Government feels that:-

- Huawei poses an unacceptable security risk.
- Justice Department indictments accused the company of stealing intellectual property and violating US sanctions on Iran.
- Huawei is beholden to a 2017 law requiring Chinese citizens and companies to assist China's security agencies in carrying out intelligence work.
- Chinese government for years has waged massive economic espionage against Western countries.
- Huawei may be installing deeply implanted flaws in the 5G network, providing Chinese intelligence services vulnerabilities to exploit.

US Action

That Huawei's products are cheap and gaining popularity across the globe worries the administration, as it suggests that the US is lagging in the global race to roll out 5G technology.

Trump administration, in executive order of May 2019, blocks Huawei products entering the US market on National Security grounds. Based on this order:-

- Google revoked Huawei's Android license. No smartphones or tablets launched by Huawei will have access to Google's Play Store and its long list of official applications.
- Huawei smartphones will not come pre-installed with Facebook, WhatsApp and Instagram.
- Intel will not sell laptop CPU.
- Chip designer ARM will not sell smart phone CPU to Huawei even though ARM is based in UK.
- All four major US network carriers - AT&T, Verizon, Sprint, T-Mobile - will not use Huawei equipment.

The US government did give some respite to Huawei phone users, giving Google a temporary reprieve of 90 days. Google is concerned it would not be allowed to update its Android operating system on Huawei's smartphones, which would prompt the Chinese company to develop its own version of the software. Google argues a Huawei-modified version of Android would be more susceptible to being hacked. Huawei has been working on its own Operating System since 2012. Huawei has applied to trademark its own mobile operating system as it prepares for life without Android. Codenamed 'Hongmeng OS', the Chinese tech giant's software would run independently of Google's Android for the first time on a Huawei smartphone.

Effects on US Companies

Huawei said Washington's decision to put the group on its entity list would affect about 1,200 American suppliers. Some of the effects are:-

- Out of $70 billon Huawei spent for buying components in 2018, $11 billion went to US firms including Qualcomm, Intel and Microtech.
- Two-thirds of the 19 commercial cyber security software tools that Huawei uses come from US suppliers.
- One-quarter of the roughly 200m smart phones it shipped last year contained chips from the US Company Qualcomm.
- The company's heavy usage of US cyber security tools, including scanning tools Nmap and Nessus, reflects American dominance in the field.

Problems of Huawei

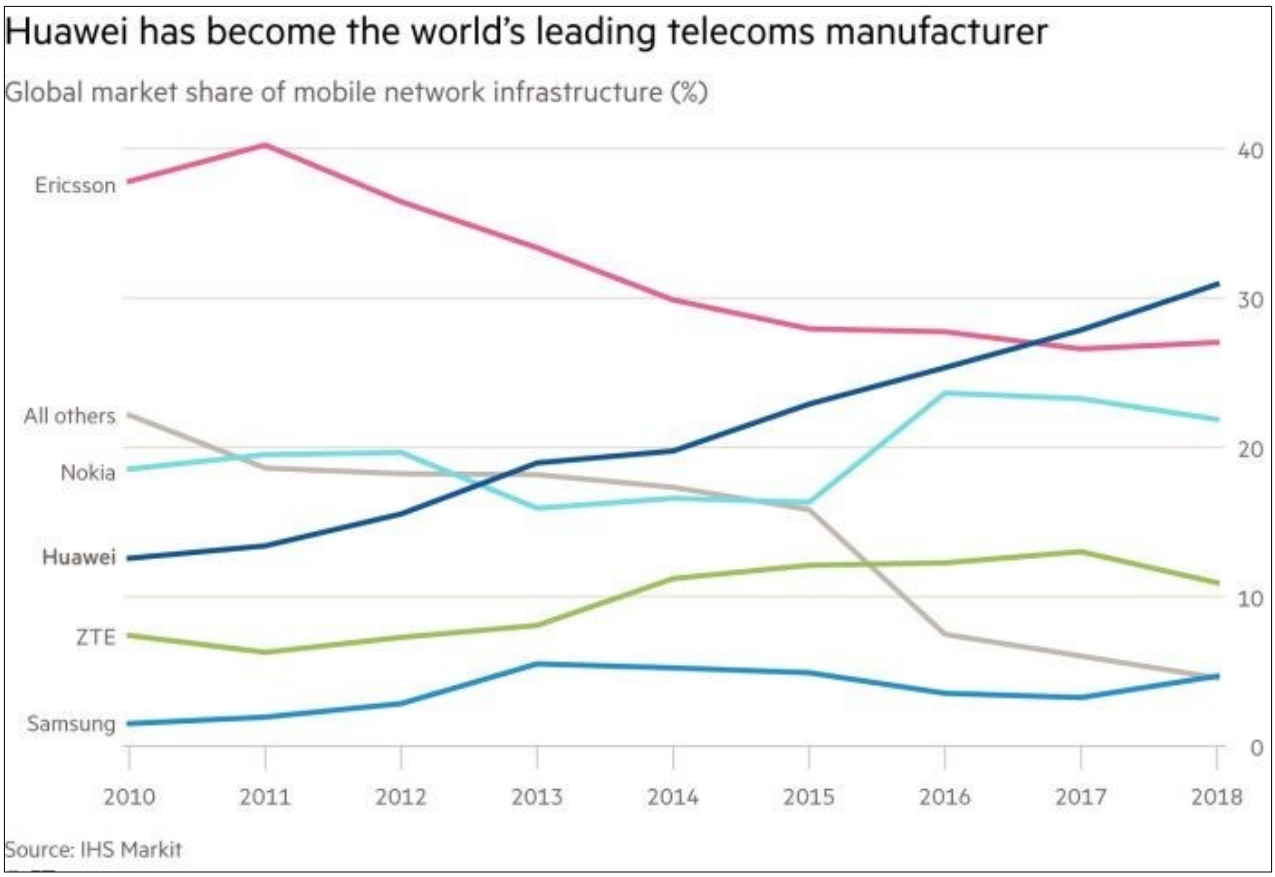
Though Huawei has anticipated and made a stockpile of US IT components used by them, clearly it is in serious trouble. Huawei has downgraded its forecast for total smartphone shipments in the second half of 2019 by about 20 per cent to 30 per cent from the previous estimate. It might lose $30 billion over the next two years. CEO Ren Zhengfei said Huawei's overseas cellphone sales will drop by 40%.

Huawei's vulnerabilities to a sudden loss of access to US suppliers include two critical areas: cyber security and semi-conductors. Intel provides chips for Huawei's laptops as well as servers, Qualcomm provides the Chinese company its processors and modems to be used in smart phones, Broadcom is a key supplier of switching chips, Xilinx offers programmable chips used in networking while ARM provides the processor of the smart phone. If the ban is fully implemented, the US government's one action could have a devastating effect on the semi-conductor industry in the short term.

Strengths of Huawei

However Huawei is a big player in telecom. It has solid support of the Chinese Government. Huawei is:-

- World leader in telecom network equipment.
- One of top smart phone manufacturer along with Samsung and Apple.
- Among the top ten most valuable technical companies by revenue, placed along Microsoft and Google. Raked $ 105 billion in 2018 alone.
- Popular in Europe, Asia Pacific, South Asia and Africa. Russia firmly sided with Huawei.
- Cheaper by at least 20-30% against its competitors.
- A huge player in infrastructure space, building submarine cables (recently hived off to another Chinese company), mobile network including 5G. It is world's leading system integrator in telecom.
- Obtained 46 commercial 5G contracts from 30 countries despite US ban.
- Shipped more than one lakh 5G stations globally.



Action by China

China's Ministry of Industry and IT granted commercial use 5G license to Huawei to start rolling 5G services. Nokia, Ericsson, Qualcomm and Intel joined 5G trials in China. China welcomed foreign and domestic companies to participate.

Huawei has sued the Trump administration over the ban and asked a federal court to rule in its favour. The Chinese Government says it expects Chinese companies to follow export control rules and observe the laws of the countries in which they do business. Huawei has denied it hacks foreign networks for commercial advantage. Huawei has said it does not build "back doors" in its products and would never help China spy on other countries. Huawei has never been caught spying. They know it would be a corporate suicide. A NATO report of 2018 said, "There has been no evidence, at least publicly, of significant vulnerability in Huawei technology"

Security Concerns of 5G

The fifth generation (5G) of mobile technologies will increase the speed of data transfer and improve bandwidth over existing fourth generation (4G) technologies, in turn enabling new military and commercial applications. 5G technologies are expected to support interconnected or autonomous devices, such as smart homes, self-driving vehicles, precision agriculture systems, industrial machinery, and advanced robotics. This would greatly increase the threat to already vulnerable IoT devices. Hackers have compromised IoT devices with massive Distributed Denial of Service (DDOS) attacks in 2016. In addition, personal data collected by thousands of IoT devices could be stolen by malicious actors. The lax security protections and universal connectivity of IoT devices create numerous points of vulnerability that hackers or malicious state actors can exploit to hold critical infrastructure, businesses and individuals at risk. These types of risks will grow as IoT devices become more complex, more numerous and embedded within existing physical structures. The size, speed and impact of malicious cyber attacks against and using IoT devices will intensify with the deployment of 5G. However, preventing Chinese hardware from supporting US networks would not make the US or its allies' next-generation networks secure. The software and applications will remain cyber security risks. Both Russia and North Korea have successfully infiltrated networks in the US without exploiting Chinese hardware.

US government lacks essential tools to conduct rigorous supply chain risk assessments. Federal procurement laws and regulations are often contradictory and are inconsistently applied. The current standard, developed by the 3rd Generation Partnership Project (3GPP), an international organisation comprised of telecommunication companies, lacks security goals and precision. The Authentication and Key Agreement (AKA), a security protocol used in 5G networks, has vulnerabilities that allow malicious actors to steal data and intercept communications. Such vulnerabilities could be exploited by foreign adversaries to attack critical infrastructures in the US The US administration does not have direct control over 5G standard-setting.

Military Implications

5G technologies have potential military applications for autonomous vehicles, command and control (C2), intelligence, surveillance and reconnaissance (ISR) systems—which would each benefit from improved data rates and lower latency (time delay). ISR systems increasingly demand high band-widths to process, exploit and disseminate information from a growing number of battle-space sensors. 5G technologies could provide commanders with timely access to actionable intelligence data, in turn improving operational decision making. Having terrestrial communications like 5G could potentially reduce latency in video and teleconferencing, thereby

improving communications and situational awareness among deployed forces. 5G could also be used to network platforms/vehicles enabling new military concepts of operations, such as swarming.

While each of these applications could increase military effectiveness, there are concerns over data security, particularly passing sensitive information like intelligence or operational requirements over commercial systems.

India's Dilemma

Rolling out of 5G has become a strategic issue for India. India is under extreme and sometimes obscene pressure from USA. China is also aggressively pushing for Huawei for induction in India's 5G network infrastructure. The cumulative economic impact of 5G on India's economy is expected to be $1 trillion by 2035 as per an Indian government study in August 2018. *5G has some very serious national security implications. But the Steering Committee on making in India 5G Ready does not have any representative from defence or intelligence community*! This imbalance must be rectified in any serious discussion on 5G.[1]

Pressure from USA

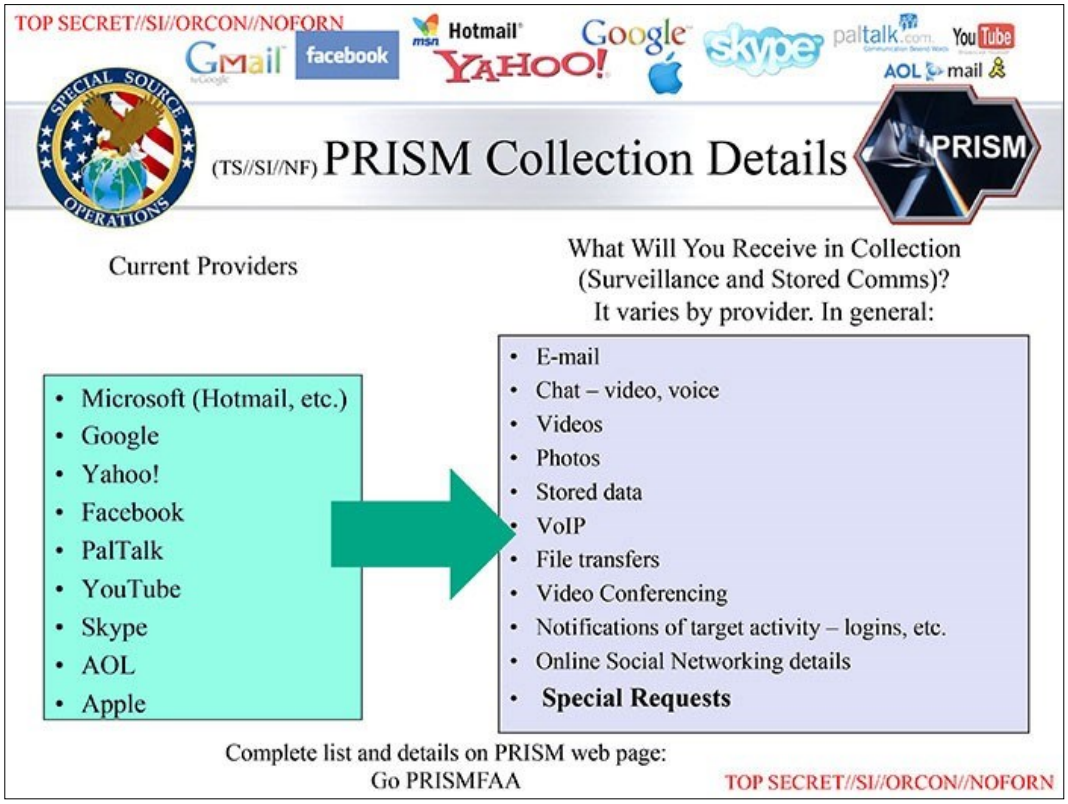
USA has made its position very clear on 5G. In the new cold war, USA is pushing the idea of 'either with US or China'. USA is pushing India hard on 5G issue. The US lobby and its considerable soft power are on overdrive. India is in a difficult situation. It is not time for hedging. India has to take side. But this has very serious repercussions on India's strategy - be it on strategic autonomy, relations with USA and China, economy and technology development. India has to consider all the relevant aspects before arriving at a decision. This would not be easy.

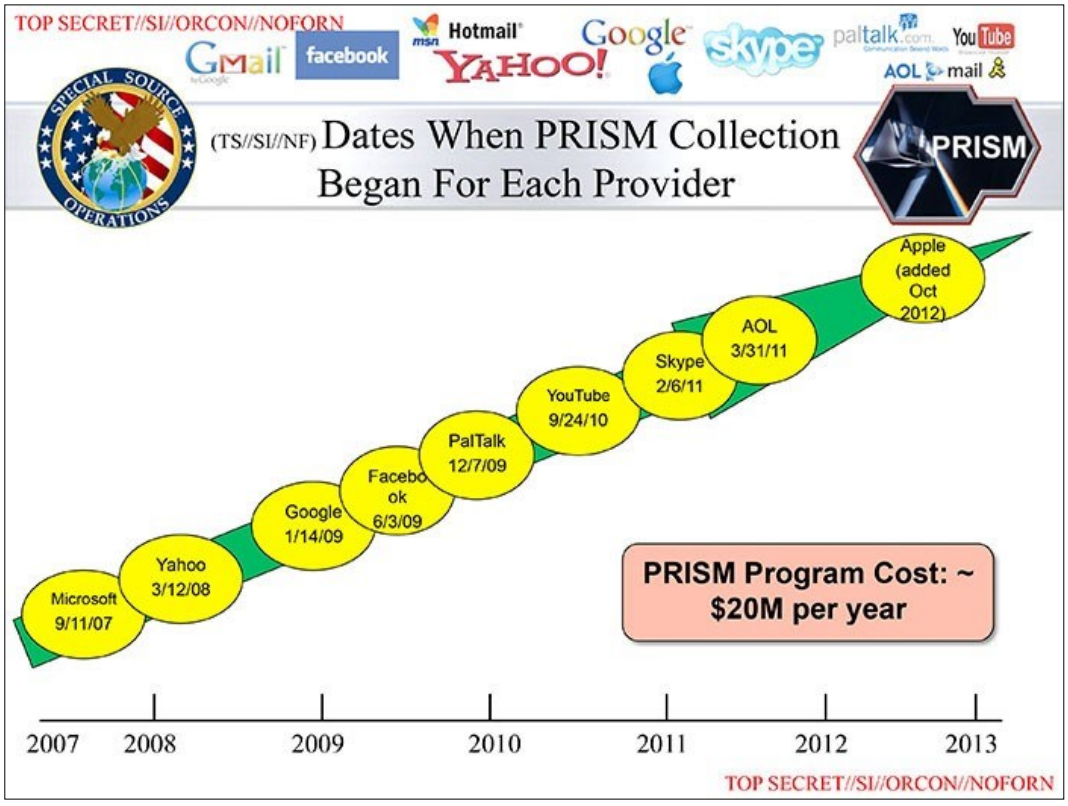
India seems to be succumbing to US pressure on Iran/ Venezuala oil issue, signing of Communications Compatibility and Security Agreement (COMCASA), Logistics Exchange Memorandum of Agreement (LEMOA) and considering favourably Basic Exchange and Cooperation Agreements for Geospatial Intelligence (BECA). On the S-400 deal with Russia, Countering America's Adversaries Through Sanctions Act (CAATSA) hangs like a Damocles Sword. As per the USA, Indo-Pacific Command spans from the West Coast of India in the Indian Ocean to the West Coast of the United States in the Pacific Ocean. India regards the whole of the Indian Ocean, stretching from South Africa to Australia as part of Indo-Pacific. The Western Indian Ocean, including the Persian Gulf, is the most strategically important sub-region of India's Indo-Pacific but it does not feature in the US' conception of the same. US wants Indian Navy to take active part in South China Sea without yielding any space in Persian Gulf, whereas India's interest lies in West of Indonesia and Indian Ocean Region (IOR).[2] USA has threatened

drastic reduction of H1B visa to India if we go ahead with our data localisation policy. All these are not good advertisement for India's strategic autonomy.[3]

Even if its security concerns against China and Huawei are true, USA does the same to other countries. Post Snowden leaks there is no doubt as to that[4]:-

- National Security Advisor (NSA) of USA monitored the phone records of Verizon.
- NSA's program of PRISM directly access the servers of US tech giants like Google, Facebook, Microsoft and Apple, among others.
- British spy agency, the Government Communications Headquarters (GCHQ), taps fiber optic cables all over the world to intercept data flowing through the global Internet.
- NSA spied on at least 122 world leaders, including German Chancellor Angela Merkel, Brazil's President Dilma Roussef, Mexico's former President Felipe Calderon, the French Foreign Ministry as well as leaders at the 2010 G8 and G20 summits in Toronto.
- NSA used XKeyscore to search "nearly everything a user does on the Internet" through data it intercepts across the world.
- The NSA used a series of techniques and tricks to circumvent widely used web encryption technologies.
- "Tailored Access Operations" (TAO), an elite hacker team hacks into computers worldwide, infects them with malware and does the dirty job when other surveillance tactics fail.
- NSA could infiltrate links connecting Yahoo and Google data centers, behind the companies' backs.
- NSA intercepted 200 million text messages every day worldwide through a program called 'Dishfire'. NSA can easily crack cellphone encryption, allowing the agency to more easily decode and access the content of intercepted calls and text messages.





(Image Source : https://nsa.gov1.info/dni/prism.html)

If the Chinese Government has control over Huawei, the US Government also has no hesitation, citing national security issues, in directing even the trillion dollar IT companies as to what needs to be done against China. Surely the ban on Huawei will adversely affect the business interests of US IT companies. Way back in 2012 the House Intelligence Committee concluded that Chinese IT companies pose a national security threat on account of spying, stealing of intellectual property and potential ties to the Chinese Government.[5] It is only now that Trump administration has taken some strong actions. The National Defense Authorisation Act – signed in August 2018 – forbids government agencies from procuring tele-communications equipment or services produced or provided by Huawei and ZTE Corporation.[6] The United States is blacklisting five Chinese organisations involved in super-computing with military related applications, citing national security as justification for denying its Asian geopolitical rival access to critical US technology. The Commerce Department called their activities "contrary to the national security and foreign policy interests of the United States."[7]

Surprisingly, there is no US major telecom infrastructure equipment provider in 5G arena. There are now only four suppliers — Nokia, Ericsson, Huawei, and ZTE. Out of these, only Huawei makes the full range of equipment. Huawei's technology is good, their prices are low and they are becoming globally dominant. The US had two major telecom equipment providers — Nortel and Lucent — but both are out of the business. Qualcomm and Cisco, while leaders in the technologies they make, do not offer the full range of equipment (such as high capacity routers) needed for the telecom backbone. Why is USA then pushing for two Nordic companies?

Under intense US pressure to force India to ban Huawei, India has not invited Huawei to participate in 5G trials to be conducted shortly. USA is not providing any alternative. Without any competition, the two Nordic companies Nokia and Ericsson will supply the whole world's 5G requirements. Prices will skyrocket. Will it work?

Huawei in India

Huawei entered India around 20 years ago and was among the first Chinese companies to invest in the country. In India, it sells products like smart phones, smart watches and dongles to retail consumers and telecom equipment and software to network carriers. Huawei's first research and development centre outside China and the largest was set up in Bengaluru. Currently, the second largest smartphone player in the world, Huawei has sensed the tough road ahead. Huawei expects India to emerge as second largest 5G market in 10 years. The company is also looking at the Indian smart phone market which has touched 450 million smartphone users and has a great potential to grow.

Huawei is keen to expand investments in India, announcing an additional $100 million. This would support Indian telecom operators already struggling with massive capital expenditure

burdens. India offers Huawei a market second only to China in size, and would be critical for its future growth.[8] Huawei has urged, "The Indian Government or any other country must take an independent view to protect its own networks and data through its own standards, test mechanisms and policies. It is important to address cyber security risks through an evidence and fact-based approach, introducing checks and balances with a monitored participation rather than banning out of fear".

Stance Taken by Other Countries

Under US pressure Australia and Japan have banned Huawei, while Canada and New Zealand are likely to follow suit. Russia, Turkey and Saudi Arabia have welcomed Huawei. Many countries in Europe are still to make a decision.

United Kingdom

In view of security concerns expressed by the UK Government and intelligence agencies, Huawei had set up a Cyber Security Evaluation Centre (HCSEC) in 2010 – an independent security testing lab – entirely at its own cost. Huawei has left no stone unturned to assure Western governments and law makers that it is not a security threat. Britain's electronic espionage agency GCHQ had set up a special cell in Banbury to examine Huawei's equipment for spyware, with the entire cost to be borne by Huawei. Recently UK National Security Council, chaired by Mrs May, concluded that Huawei could build some parts of Britain's 5G networks, but the move was subject to a final decision by the government.

UK Government has signaled their willingness to take a middle road — barring Huawei components from their networks' 'core', which they consider sensitive because it contains the routers and switches that handle massive volumes of traffic, but allowing them in some portion of the '"edge', which comprises what they say are the less sensitive radio antennas that carry signals to the core from phones and other devices. But US officials argue that in 5G, the antennas will become ubiquitous and carry more computing power. Housed in cases the size of pizza boxes and affixed to street poles and buildings, these will enable super-speedy connections to all manner of devices — smartphones, highway traffic sensors, virtual reality goggles. The distinction between the core and edge has eroded with 5G, and Huawei must be banned from the entire system.

Europe

European states like France and Germany have refrained from an outright ban on Chinese telecom operators, arguing that the risk can potentially be managed through a mix of regulation and technological solutions. Their approach is a product of a mix of economic and political

considerations, such as switching costs, the cost effectiveness of Huawei products and the desire for strategic autonomy. The Huawei issue has provided a competitive advantage for European rivals such as Ericsson and Nokia. Sweden's Ericsson has already rolled out nine live 5G networks globally. There will be increasing pressure on Nokia and Ericsson to fund a security initiative on par with the Huawei Cyber-security Evaluation Centre. This is an expense neither would want to make unless forced, but it is a possibility.

Deutsche Telekom came out with a paper cautioning governments in Europe that disallowing and banning Huawei equipment from the 5G network in Europe is going to severely hinder the ability of a European company to roll out 5G technologies across the continent. What are the alternatives? How should it be done? Is it a government driven effort, or should it be public private partnership?

India's Options

The size of the Indian market is crucial economic leverage that must be used to achieve strategic objectives. The higher the stakes in the Indian market, the greater the potential political leverage for India. Control over such investments provides the Indian state an economic tool to achieve political and strategic objectives. The Indian Government must keep this in mind while framing rules attracting foreign investment and regulating the participation of foreign firms in the telecom sector.

India has not been very good in leveraging its market. When Microsoft went to China, China demanded the codes before giving permission to enter its market. Despite the huge market, India did not ask for anything. It is only after Microsoft gave the codes to China it offered the same to us. In 2009, the State-run telecom giant Bharat Sanchar Nigam Limited (BSNL), in spite of strong opposition from the Intelligence Bureau (IB) and the defence ministry, awarded the contract for telecom equipment to Chinese company Huawei for only southern states. The logic given was that Southern India does not share sensitive borders with countries such as Pakistan, China and Bangladesh as they have no international land borders. In today's networked world this logic is weak.

Most of India's telecom sector players including the state owned BSNL to Reliance have been using Huawei equipment for more than a decade because it is cheap and the telecom companies get favourable financial loans from Chinese banks. The security concerns were always there. The narrative used to be given was: we are signatory to the World Trade Organization (WTO), preventing Chinese companies would invite WTO sanctions. None of these conditions have changed. In fact, it is the USA which has made the WTO's Appellate Body non-functional. On December 11 this year when two of the remaining three members' terms expire, it will no longer have enough members to conduct appeals and will effectively go out of business.

Indian Government has made its position difficult by not taking any policy decision on introduction of Chinese IT companies like ZTE or Huawei in India's backbone network infrastructure. In the absence of any such policy the Huawei network equipment are now part of India's BSNL and private telecom networks, and alarmingly, in the classified defence services' networks. While nothing has changed as far as India is concerned, now to ban Huawei under US pressure puts Indian government in poor light. India imports mostly its telecom equipment requirements from foreign vendors. In Financial Year 2018 India's import bill for telecom equipment was $21.85 billion. Espionage and surveillance concerns will remain high. Surveillance and espionage by outside agencies in all probability will happen. Actual Issue is a matter of who is trusted more: the US or China.

India-China relationship is riddled with deep strategic mistrust. India has fought a war with China. The land boundary dispute between the two countries remains unresolved. In 2006 the Chinese ambassador to India claimed that all of Arunachal Pradesh region is Chinese territory. China has constructed road in Demchok and Doklam to create tension between the two countries. Chinese capacity build-up and construction activity, not just along the Line of Actual Control (LAC) but also in sensitive regions such as the Doklam Plateau continue despite the tense 2017 standoff and Xi-Modi informal summit at Wuhan. China has been using Pakistan to contain India effectively. China's engagement in Pakistan via CPEC is a reminder of Beijing's disregard for India's concerns regarding the violation of its sovereignty and territorial integrity. China's deep military ties with Pakistan along with the diplomatic cover it provides for Pakistan based terrorists are testimonies of China's intentions.

Huawei is different from other vendors like Nokia, Ericsson or Samsung and the decision on it must be viewed from the prism of the broader threat of not just espionage and surveillance but also disruptions of systems during a bilateral crisis. The decision on what role of Huawei, if at all, in building India's 5G network infrastructure has to be taken after conducting a cost benefit assessment, given the nature of the bilateral relationship.[9] It is in India's interest to create a level playing field for all possible equipment vendors, including Chinese manufacturers. Greater competition will increase the quality and reduce the price of the equipment acquired. While there should be no outright ban on Chinese vendors, their participation should be restricted, conditional and tightly regulated.[10] Huawei and other Chinese vendors should be excluded from providing equipment for or participating in building and maintaining core and critical 5G infrastructure. Participation by Chinese vendors should be encouraged in non-critical sectors and end user and consumer markets, fuelling the connectivity of India's economic hinterland to the digital economy, given the affordability and competitiveness of their products.

India's 5G network infrastructure must not be overly reliant on any one vendor. Being locked in to one vendor has significant economic, security and political costs. Telecom operators should

work with a mix of vendors along with a focus on 'fail safes', redundancies and backups of varying degrees of sophistication to increase resilience. There is the requirement of different standards for different kinds of networks - national security, critical national infrastructure and general connectivity. They do not all have to be equally integrated to the overall network and should have the ability to function independently in the event of a crisis. India may explore cooperating with countries having advanced technologies like South Korea and Japan to develop 5G technology. NEC of Japan has already set up a Lab at Delhi in cooperation with IIT, Mumbai.

Unfortunately India does not have its own telecom equipment manufacturer. Hiding behind the garb of WTO India failed to back its own companies like Tejas Networks Ltd, one of India's largest domestic telecom equipment firms. Security can only be ensured by indigenous technology. Digital India and Make in India must address development of indigenous network equipment capability.

Spectrum Management

The Government has officially pushed the potential auction to August 2019. While the frequencies which are already being used globally for the rollout of 5G technology fall in the 3.5 GHz range, these are yet to be auctioned in India. Because of expected huge revenues to the governments there will be intense pressure to release defence spectrum. One can safely visualise the use of electro-magnetic spectrum in the recent Balakot air operations by different platforms for use of weapons, communications, radars, C4ISR etc. Often it is suggested by the officials, since the electro-magnetic spectrum is not in use in peace time, this can be used for commercial purposes and would be handed over during operations. But it is exactly for operational reasons that the spectrum is never used during peace time. The interests of defence services in frequency spectrum for operational purposes must be taken care of.[11]

Conclusion

Kiron Skinner, Director of Policy Planning for the US Department of State while Addressing the annual Future Security Forum, a foreign policy seminar on global challenges sponsored by the New America think tank in last week of May this year in Washington discussed the Trump administration's outlook on the unique "long-term threat" presented by China, which is "a fight with a really different civilization." She said the decades long Cold War between the US and the Soviet Union "was a fight within the Western family." She described today's US-China conflict as "a fight with a really different civilization and a different ideology, and the United States hasn't had that before. The first time that we will have a great power competitor that is not Caucasian." Skinner was a professor of international relations and politics at Carnegie Mellon University in Pittsburgh, Pennsylvania, before joining the administration. A series of noted heavyweights have held Skinner's job, the only foreign policy think tank post within the federal

government, including Paul Nitze, Richard Haass and George Kennan. Though controversial her comments cannot be taken lightly.[12]

Data is the key, new currency, and the US controls the world by its superior technology. China's influential "Internet Plus" and "Made in China 2025" initiatives seek to capitalize on the rise of integrated digital technology and automation to transition China's economy to higher-value-added manufacturing and services and transform China into a technological powerhouse. China is fast catching up, though there is a substantial technology gap. But the gap is closing. USA the only superpower will not like a competitor to challenge its hegemony. It will take all possible measures to halt China's technology progress.

India has to be very careful. Unfortunately India has only its huge market as the leverage. The 5G and Huawei is not a technical issue, it is a complex strategic issue. Huawei is already inside India's backbone network. Its network equipment are part of India's armed forces classified networks. But by banning Huawei India's security concerns are not eliminated. India should look at what the other countries specially the Europeans are doing. India is in no hurry. India should follow a wait-and-watch policy and should not commit anything now in spite of extreme US pressure.

References:

1. The Steering Committee. "Making India 5G ready" 5G High Level Forum. August 23, 2018 available at : http://dot.gov.in/sites/default/files/5G%20Steering%20Committee%20report%20v%2026.pdf?download=1
2. Walter C. Ladwig III and Anit Mukherjee The United States, India, and the Future of the Indo-Pacific Strategy , June 20, 2019, available at , https://www.nbr.org/publication/the-united-states-india-and-the-future-of-the-indo-pacific-strategy/
3. Maj Gen P K Mallick, VSM (Retd), 2+2 Dialogue and Indo US Relations, Vivekananda International Foundation, October 2018 available at : https://drive.google.com/file/d/1HFIpCaVOYtqqdRb8-x45Xz45We5Xp5mJ/view
4. Lorenzo Franceschi and Bicchierai, The 10 Biggest Revelations From Edward Snowden's Leaks, JUN 05, 2014 available at : https://mashable.com/2014/06/05/edward-snowden-revelations/
5. Mike Rogers and Dutch Ruppersberger, "Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE", US House of Representatives – 112th Congress, October 08, 2012.
6. "H.R.2810 - National Defense Authorization Act for Fiscal Year 2018", US Government Publishing Office, December 12, 2017.
7. US Commerce Department Blacklists 5 Chinese Military-Related Supercomputing Organizations, June 22, 2019, available at : https://www.news18.com/news/world/us-commerce-department-blacklists-5-chinese-military-related-supercomputing-organizations-2198923.html

8. Cong Wang, Huawei's India investment plan to address local concerns, create jobs: analysts, Global Times, October 21, 2018, available at : http://www.globaltimes.cn/content/1123851.shtml
9. Manoj Kewalramani and Anirudh Kanisetti, 5G, Huawei & Geopolitics: An Indian Roadmap Discussion Document 2019-04, Takshashila Institution, 19 June 2019, available at : https://takshashila.org.in/takshashila-report-5g-huawei-geopolitics-an-indian-roadmap/
10. Nitin Pai, As China Fights For Huawei, Should India Be Wary of Its 5G Entry?, The Quint, 24 January 2019, available at : https://www.thequint.com/voices/opinion/china-fights-huawei-should-india-be-wary-of-its-entry-in-5g
11. Press Trust of India, "DoT Expects to Complete Process for 5G Spectrum Auction by August 2019", Business Standard, December 17, 2018, available at : https://www.business-standard.com/article/economy-policy/dot-expects-to-complete-process-for-5g-spectrum-auction-by-august-2019-118121700468_1.html
12. Minxin Pei, Is Trump's Trade War with China a Civilizational Conflict? May 14, 2019,available at : https://www.project-syndicate.org/commentary/trump-race-war-against-china-by-minxin-pei-2019-05

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