ORF OCCASIONAL PAPER
226
DECEMBER 2019

# 5G Infrastructure, Huawei's Techno-Economic Advantages and India's National Security Concerns: An Analysis

Gautam Chikermane

ORF OBSERVER RESEARCH FOUNDATION

# 5G Infrastructure, Huawei's Techno-Economic Advantages and India's National Security Concerns: An Analysis

Gautam Chikermane

ORF OBSERVER RESEARCH FOUNDATION

## ABOUT THE AUTHOR

**Gautam Chikermane** is Vice President at Observer Research Foundation. His area of research is economic policy.

ISBN: 978-93-89622-13-3
ISBN Digital: 978-93-89622-11-9

# 5G Infrastructure, Huawei's Techno-Economic Advantages and India's National Security Concerns: An Analysis


## ABSTRACT

China's Huawei, a global leader in providing equipment for fifth-generation (5G) mobile technology, is attempting to enter the Indian market. However, in light of China's proclivity for state interference in corporate operations and the critical infrastructure Huawei deals in, the firm poses a security threat for countries with its presence. This threat gets amplified for India, when seen in the context of China's anti-India stance on a range of issues, a Chinese law that binds corporations to collect and share intelligence, and the 3,488-km-long volatile India–China border. This paper analyses the legal, geopolitical, strategic and technological risks of allowing Chinese firms such as Huawei into India's critical infrastructure. Weighing the transformative force of 5G against India's national security requirements, it provides six policy contexts within which to examine this complex issue.


*(This paper is part of ORF's series, 'Eye on China'. Find other research in the series here: https://www.orfonline.org/series/eye-on-china/)*


Attribution: Gautam Chikermane, "5G Infrastructure, Huawei's Techno-Economic Advantages and India's National Security Concerns: An Analysis", *ORF Occasional Paper No. 226*, December 2019, Observer Research Foundation.

## INTRODUCTION: SECURITY FIRST

Fifth-generation (5G) wireless communication is likely to be one of the most crucial transformative tools of the 21st century, impacting the economy, society, cities and security. The Chinese company Huawei is one of the providers of 5G equipment, over which this technological transformation will ride. However, it is not merely a private company operating within the rules of Indian law to deliver services. Huawei's technological prowess and low-cost products hide an invisible price: the threat to India's national security. Chinese laws obligate Huawei to collect intelligence from the countries it operates in and share that information with the Chinese state. Thus, there is a substantial risk associated with a Chinese firm delivering critical infrastructure. The risk is amplified in India's case due to China's open hostility towards India in most international forums; the long and conflictual geographical border the two countries share; and China's closeness with Pakistan, a country that uses terror as state policy against India. It is in this geopolitical, strategic, defence and security context that Huawei's entry into India needs to be seen.

Using Huawei as a case study, the intrusive nature of the Chinese state as background, and the increasingly hostile stance of China against India as a defining vector, this paper argues that despite their compelling economics, no Chinese firm should be allowed into India's critical infrastructure. The paper is divided into ten sections.

Section 1 outlines the power of the 5G technology, explores how it is critical to nations, and places the context within which to evaluate firms that manufacture and sell 5G equipment in India. Section 2 shows how a company called Huawei is besieged by a risk called China. As a firm that stands on the cutting edge of technology and offers it at low cost, Huawei is a logical choice as a back-end equipment provider for any

telecommunications firm. Had the company's nationality been of any other friendly country wanting to do business in India and with India, Huawei would be as welcome. Section 3 elaborates specific risk in the form of China's National Intelligence Law that Huawei is legally bound to follow. Section 4 observes that China's foreign policy in general, and on India in particular, is motivated by its 'century of humiliation', and argues that the country is possibly weaponising shame. Section 5 explores where other countries stand in allowing, banning or fence-sitting around Huawei. Section 6 captures how the trust deficit between India and China prevents India from allowing Huawei to enter and deliver critical infrastructure. It also addresses the attempts by the leaders of the two nations to build trust bridges. Section 7 studies the rise of nationalism across the world, including in China and India, and its implications for businesses, consumers and investors. Section 8 examines the accentuated security concerns to India due to a 3,488-km-long border with China, fraught with military frictions and strategic tensions. China's intentions being clear, this geography underlines and powers all other arguments against the entry of Huawei into India. Section 9 offers six policy contexts within which India should examine the entry of Huawei. Section 10 concludes the paper, retaining the opening proposition that under current circumstances, India cannot and must not allow any Chinese firm to participate in or deliver critical infrastructure.

## 1. THE POWER OF 5G TECHNOLOGY

Considering the growing significance of 5G communication and the benefits it offers, this technology is classified as "critical infrastructure." Critical infrastructure comprises those whose destruction would adversely impact a country's security, economy or safety. It could be physical (roads, ports, energy, railways); virtual (information technology, internet, broadband); systemic (banking, finance);

networked (telecommunications); and other areas (space, nuclear, public health). In India, such infrastructure is created and managed in partnership between the government and the private sector through public-private partnerships (PPP). Critical infrastructure requires the government to identify risks and vulnerabilities—natural or otherwise—and be prepared for them.

The criticality of 5G and the risk-management systems, both physical and policy, the government will need to build will be exponential going forward. The 5G cellular network system is a tool that will support always-on firms, highly mobile consumers and, above all, fully-connected societies. This technology will sit at the centre of the fourth industrial revolution (4IR), the Internet of Things (IoT), smart cities and self-driven cars. The 5G network could carry a throughput of data, up to 100 times that of 4G.[1] Essentially, this technology enables complex networks to seamlessly interact with each other. 5G can be visualised as a network of networks.

The evolution from 0G to 5G has been a trajectory of technology as much as of applications and consumer empowerment. Based on a timeline provided by Firooz B. Saghezchi et al.,[2] the technology of telecommunications has generally advanced every four to 14 years: seven years from 1G to 2G, five years from 2G to 2.5G, four years from 2.5G to 3G and 14 years from 3G to 4G. It is estimated that the shift from 4G to 5G should take approximately eight years, and 5G will be ubiquitous across the world by 2021. The shift from 4G to 5G is not merely about the speed of downloads, though speed is an essential component of what it can deliver. According to the International Telecommunication Union (ITU),[3] the framework for the development of the International Mobile Telecommunication (IMT) 2020 standards takes 5G into account, with a spectrum efficiency that is expected to be three times higher (with very low over-the-air latency) and will support

high-speed trains or Massive Machine-Type Communication (mMTC) scenarios,[4] characterised by a large number of connected devices transmitting relatively low volume of non-delay sensitive data, useful to cover IoT, smart agriculture, smart cities, energy monitoring, smart home and remote monitoring.[5]

However, it is what 5G enables that makes the technology as lethal to its users as it is beneficial. In the near future, 5G is set to become the backbone of smart cities and IoT. Through enhanced mobile broadband, the technology can deliver augmented- and virtual-reality functionality. It can enable climate-smart agriculture, smart cities and smart homes through MMTC. It can drive autonomous vehicles, smart grids, remote patient monitoring and telehealth, and industrial automation through ultra-reliable and low-latency communications,[6] all of which depend on the ability of 5G technology to support, link and power the IoT. The IoT has been defined by D. Minoli and B. Occhiogrosso:[7]

> "The basic concept of IoT is to enable objects of all kinds to have sensing, actuating, and communication capabilities, so that locally-intrinsic or extrinsic data can be collected, processed, transmitted, concentrated, and analysed for either cyber-physical goals at the collection point (or perhaps along the way), or for process/environment/systems analytics (of predictive or historical nature) at a processing centre, often 'on the cloud'. Applications range from infrastructure and critical-infrastructure support (for example smart grid, smart city, smart building, and transportation), to end-user applications such as e-health, crowdsensing, and further along, to a multitude of other applications where only the imagination is the limit. Some refer to the field as 'connected technology'. While the reach of IoT is (expected to be, or become) all-encompassing, a more well-established subset deals with Machine-to-Machine (M2M)

> communication, where some architectural constructs and specific Use Cases have already been defined by the standardisation community."

According to Saghezchi et al., 5G technology is still evolving:[8]

> "5G is still to be defined officially by standardisation bodies. It will be a system of super high capacity and ultra high speed data with new design requirements tailored towards energy elicited systems and reduced operational expenditure for operators. In this context, 5G envisages not only one invented technology, but a technology ecosystem of wireless networks working in synergy to provide a seamless communication medium to the end user. Thus, we can say that moving from 4G to 5G means a shift in design paradigm from a single discipline system to a multi discipline system."

What is this ecosystem? The complexity of 5G technology is such that it needs highly specialised world-class expertise and equipment for its various components. Huawei, for example, procures only some components from its home country, China. These include cameras, laser amplifiers and batteries. It sources antennas, data storage, modems, software and licences from the US; semi-conductors from Germany, Netherlands, Switzerland or Taiwan; and memory cards and display panels from Japan. Since the US placed a ban on doing business with Huawei, the company has had to look elsewhere to source several essential components.[9]

Of significance here is the fact that the intricacy of 5G technology requires equipment providers to source components from a variety of countries and companies (as Huawei does), and these sources include Chinese manufacturers. Thus, even if India were to ban Huawei or

Chinese firms for 5G, some Chinese components may still find their way into the Indian market through other vendors. For example, radar sensors are an important component for remote medical diagnosis and surgery, vehicle-to-vehicle and vehicle-to-infrastructure communication for self-driving cars, smart transportation and smart industry. This is a market that Huawei is attempting to enter,[10] and its ecosystem comprises chip designers, component manufacturers, technology providers and system integrators. Companies that make them are spread across Germany, Japan, UK, Netherlands, the US and Sweden. The job of radar-sensor manufacturers, therefore, involves getting the best components from across the world and assembling them. The question that arises then is this: What will be the effective 'country of origin' of such a product that, like an Apple iPhone, may have components from companies from all over the world? Conversely, what is the guarantee that 5G equipment from Sweden's Ericsson, South Korea's Samsung, Finland's Nokia or the US' Cisco will not carry components from China's Huawei or ZTE? One way forward is to simply rely on the fact that the final assembling, and thus the control and accountability, will be in the hands of a non-Chinese firm and therefore subjected to democratic scrutiny and justice, not to the whims of an authoritarian China.

As a critical telecommunications infrastructure that is global, 5G can deliver a boundless, high-speed, reliable and secure broadband experience; create innovative future networks; provide the networks and platforms to drive the digitisation and automation of industrial practices and processes (including the 4IR); and power the IoT and critical communications services.[11] It can also bring societal changes—individual, corporate, regulatory and governmental. 5G will be to the 21st century what computers and satellites were to the 20th century and steam engines to the 19th century. Through IoT, this technology is expected to fundamentally transform the role that telecommunications plays in our lives, not only delivering a future where all people are

connected to one another, but also creating a society where everything and everyone is connected.[12]

While the benefits of 5G are unimaginable, those driving the technology can also wreak havoc that on governments, citizens, financial flows and businesses, at a scale unprecedented and through an intrusion unmatched. In light of this, to hand this infrastructure to a foreign company (Huawei) that is bound by law (See Section 3) to support its nation of origin (China) on matters of intelligence-gathering is to expose India to tremendous risk.

Imagine the potential destruction if self-driven cars are sent distorted signals, long-distance operations sent incorrect images, traffic lights in smart cities manipulated to create accidents, communications infrastructure for airlines or railways disrupted, business secrets of rival firms culled out, fake news narratives created. Above all, imagine the possibility of injecting spyware into the security infrastructure or into financial systems of stock, currency or commodity exchanges, all of which would be acts of war. In repeated tensions along borders or in support of Pakistan's terror, any or all of these would be tools in the hand of the Chinese government to destabilise India and its national interests.

No government, no political party, no regulatory structure and no security system the world over can accept this level of risk for its citizens. Preventing the entry of Huawei can be visualised as a technological policy vaccination.

## 2. A COMPANY CALLED HUAWEI IN A RISK CALLED CHINA

In China's context, commercial actors are an extension of the government, which in turn is openly and brazenly hostile to India. Against this background, Huawei's entry into the Indian market will be

tantamount to infiltration by the Chinese state. Although India's stance is clear, its actions are not, evident in the fact that it is yet to ban Huawei.

According to Huawei's official statement, the company has no links to the Chinese state. Addressing a series of questions to explain its position, here's what the company states:[13]

> "Has Huawei received requests for intelligence information?
>
> No, Huawei has never received any request to add backdoors or spyware to its systems. Even if such a request was made, it would not be possible for Huawei to comply, as Huawei does not own or operate these networks nor does it have access to these networks in the U.S."
>
> "Has Huawei worked with Chinese intelligence?
>
> No, Huawei does not work with Chinese intelligence and never has. Doing so would run contrary to our commitment to our customers, and Huawei would never betray that trust."
>
> "What is Huawei's relationship with the Chinese government?
>
> Huawei is a private company, owned solely by our employees. No third parties hold any shares in the company, and that includes the Chinese government.
>
> We are a global company that works openly and transparently with the governments of 170 countries where we do business. We have commercial agreements in place with these governments, and this includes China. We sell civil communication products to the Chinese government, and that is the extent of the relationship."

However, US intelligence allege that the Chinese government has helped finance Huawei,[14] in addition to enabling intellectual property theft.[15] Further, according to new revelations by CIA,[16] Huawei has taken money from the People's Liberation Army, China's National Security Commission and a third branch of the Chinese state intelligence network. On 28 January 2019, the US Department of Justice indicted the company for theft of trade secrets, wiretaps and obstruction of justice.[17] Following this, on 16 May 2019, Huawei was added to the 'Entity List' of the US Department of Commence (US Bureau of Industry and Security).[18]

From a pricing perspective, Huawei's prices are highly competitive and affordable, according to industry analysts.[19] From a technological standpoint, Huawei has the highest number of 5G patents (followed by Nokia, and Samsung and ZTE) and makes the highest number of technical contributions to the 5G standard (followed by Ericsson, Hisilicon and Nokia).[20] Such is the technological prowess of Huawei that despite US President Donald Trump's administration putting a ban on Huawei in May 2019, the company unveiled a new operating system for its phones to replace Android in less than four months.[21] However, Huawei's competitive advantage needs to be seen in the broader context of a constantly improving technology on the one side and constantly reducing prices on the other. Its lead, therefore, could be short-lived in a world of globalised competition. Its low prices will compel other network service providers to lower their rates, giving buyers more options to make informed choices. Thus, it will not be long before competitors such as Sweden's Ericsson, Finland's Nokia, South Korea's Samsung and China's ZTE catch up with Huawei's technological competency as well as affordable prices. The opening up of the global market, as countries inevitably and successively adopt 5G into their communications networks, should also deliver economies of scale.

Currently, Huawei's competence and its ostensibly harmless presence in other countries lend it a substantial appeal. With US$105 billion in revenues, which have increased at a compounded annual growth rate (CAGR) of 26 percent over the past four years; US$10.7 billion in operating profits (CAGR: 21 percent); and US$8.3 billion in net profits,[22] Huawei is an entrepreneur-led firm that has taken huge strides to become the world's largest telecommunications company across the value chain—from handhelds to networks. Further, it won half of the state-owned China Mobile's 5G contracts in China in June 2019[23] and provided the equipment for the recent launch of 5G services in Beijing and Shanghai.[24]

In over 30 years of existence, Huawei has won 46 commercial 5G contracts in 30 countries[25] and has operated in 170 countries,[26] including India. It is the world's second-largest smartphone manufacturer,[27] after Samsung. In December 2018, Huawei broke "golf club relationships" to become the world's largest telecommunications equipment manufacturer.[28] The company runs the telecom networks of the United Kingdom,[29] Russia[30] and 60 percent of Europe.[31] Such a size and global footprint cannot come solely by riding a single competitive advantage of state support. It needs technical innovation, on-ground delivery and consistency of service.

But Huawei's accomplishments pale into insignificance due to its Chinese nationality. Along with ZTE, Huawei sits on the Chinese government review boards, which tested and approved foreign telecommunications equipment for the large, growing and underserved Chinese market. "Sitting on these boards, Huawei and ZTE learned how to copy foreign designs while testing and opening the equipment of foreign vendors as part of the approval process."[32] Thus, Huawei has benefitted tremendously from the Chinese state. Now that the company

has grown and is self-reliant, it would be naïve to assume that the Chinese government will not reap the benefits in return, in areas such as foreign policy and intelligence gathering.

Huawei's presence in India, therefore, poses three major risks. First, G2G (government to government, or the direct threat that the Indian state faces from the Chinese state). Second, B2B (business to business, or the risk that Indian companies face when dealing with Chinese companies that serve the interests of the Chinese state). And third, B2C (business to consumers, or the risk that Indian consumer-citizens indirectly face when using products made by Chinese companies that are beholden to the Chinese state). The greater data speeds and the multitude of applications that a 5G network allows citizens, businesses and governments enable them to negotiate a whole new world of robotics, artificial intelligence, self-driven vehicles, smart cities, power networks, defence and banking. However, once a network is employed for a particular technology, the costs of changing it are huge (visualise the shift from an iOS to an Android or an Apple computer to a Dell and multiply the time and investments exponentially). China's legal and political environment, along with its well-known PPP model of cyber espionage,[33] are areas of concern, wherein private Chinese actors could potentially be used to deliver state objectives.

## 3. CHINA'S INTELLIGENCE-SEEKING LAWS

By law, Chinese companies are required to cooperate with their government in supporting the country's national interests, including participation in intelligence activities.[34] According to an RWR Advisory Group Report from 13 February 2018, China's new law appears to create sweeping obligations to the state, for otherwise private citizens and companies: "The issue of Huawei 5G deployment must be assessed in the

broader geopolitical context."[35] China's strategy of systematic technology acquisition and diversion exemplifies the close relationship—within this context—between its private companies and the Chinese government. Following are excerpts from remarks of a US government official, Christopher Ashley Ford, Assistant Secretary, Bureau of International Security and Non-Proliferation:[36]

> "Huawei is also an important player in Beijing's ongoing military-civil fusion effort to make available to the Chinese military any and all technologies it wants from among those to which the country's civilian sector may have access.
>
> ...products and technologies from Huawei, Tencent, Alibaba, Xiaomi, Lenovo, and other companies have already been used in the research, production, and repair of weapons and equipment for the PLA. These companies have also provided support services for China's military industry in areas related to electronics, aerospace, shipbuilding, and weapons — all of which, incidentally, are key military-civil fusion target areas when it comes to foreign technology acquisition — to enhance the core competitiveness of China's national defence science and technology sectors.
>
> China's military-civil fusion highlights the troubling lack of any clear separation between government, national strategies for military modernisation, and the companies that are implementing and enabling those strategies to succeed.
>
> ...it is, by design, increasingly difficult to separate where commerce ends and the government begins."

A quick reading of the National Intelligence Law[37] (NIL) of the People's Republic of China (adopted at the 28th meeting of the Standing

Committee of the 20th National People's Congress on 27 June 2017) lends weight to the argument that no country should allow Chinese companies in their critical infrastructure.

*[Note: the law has been translated by China Law Translate, a collaborative translation project. Excerpts from the law; inferences author's.]*

> "**Article 7:** All organisations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of."
>
> *Inference: All Chinese companies and individuals are bound by law to support China's intelligence agencies.*
>
> "**Article 9:** The State gives commendations and awards to individuals and organisations that make major contributions to national intelligence efforts."
>
> *Inference: There are incentives and benefits for companies and individuals that make contributions to national intelligence efforts.*
>
> "**Article 12:** In accordance with relevant State provisions, national intelligence work institutions may establish cooperative relationships with relevant individuals and organisations, and retain them to carry out related work."
>
> *Inference: Chinese companies and individuals may receive intelligence work from Chinese intelligence agencies.*
>
> "**Article 14:** National intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organs, organisations, and citizens provide necessary support, assistance, and cooperation."

*Inference: Chinese intelligence agencies have the right to 'request' companies to support, assist and cooperate in their intelligence efforts. However, these 'requests' turn into 'shall support', which are legally binding requirements, as evident when Article 14 is read in conjunction with Article 7.*

A report by the Sweden-based law firm Mannheimer Swartling clarifies this further.[38]

> "NIL applies globally to Chinese Groups, whereby all subsidiaries, even those outside China could be subject to NIL. Because the Chinese parent company is subject to NIL, NIL could, from a public international law perspective, also have jurisdiction over the group's foreign subsidiaries. In addition, the Chinese parent has governance powers over foreign subsidiaries, which could enforce their compliance with NIL. [...] NIL applies to all organisations in China, a term which appears to include all types of companies established in China, regardless of ownership, i.e. private and public Chinese shareholders as well as foreign shareholders. [...] NIL applies to all Chinese citizens, and because NIL does not appear to have an explicit geographical limitation, it could be construed to apply to all Chinese citizens even when residing outside of China."

Huawei, of course, denies these allegations[39] and claims that the world is misreading the NIL. According to Huawei officials, Chinese laws do not compel the company to install "backdoors" in its infrastructure. They deny ever having worked with Chinese intelligence. While Huawei has admitted that its founder, Ren Zhengfei, is a member of the CPC, they insist that this has no bearing on the business. "When Ren Zhengfei was a young man, you needed to be a CPC member to have any position of responsibility, even as the head of a cooking team in the military." The

banality of this statement aside, it shows how deeply the Chinese state infiltrates the innards of its citizens' and companies' lives.

At a political level too, there are tangible risks. The Communist Party of China (CPC) has cells established in all large Chinese firms, as Huawei concedes.[40]

> "Does Huawei have ties to the Communist Party of China (CPC)?
>
> Chinese law states that Chinese and foreign companies operating in China must set up CPC committees. In accordance with this law, Huawei had set up a CPC Committee. Our CPC Committee is not involved in any operational or business decisions."

Officials of the party are known to participate in the policymaking for these firms. According to a *Financial Times* report, "Government of the Chinese tech hub of Hangzhou is assigning officials to 100 local companies including tech group Alibaba, in the latest example of a tightening of the ties between the state and private sector."[41] If the Chinese state and the major political party have such deep ties with private firms, it not only tilts the competitive scales against private firms from other countries but, in the case of Huawei delivering 5G critical infrastructure, increases the risk for consumers, citizens and states using its equipment.

## 4. HUMILIATION AS CHINA'S CURRENCY OF GLOBAL DISCOURSE

Obsessed with its 'century of humiliation', China remains a nation driven by shame. In the process, it has weaponised shame, both as an instrument of attack and a shield of defence. It uses shame as a tool for aggressive and confrontational nationalism that emphasises the trauma the country suffered at the barbaric destruction and full-scale

looting of Yuanmingyuan, the palace of the emperor of the Qing dynasty, in October 1860. The Japanese occupation of China during World War II was deliberately brutal and sadistic: millions were terrorised, tortured and murdered.[42] However, that Xi Jinping not only continues to carry this shame but has integrated it in China's political discourse shows that perhaps this country will never be able to rise above its victim mentality. In effect, Xi Jinping has hijacked the CPC and created a narrative to serve his personal ambitions, transforming humiliation into a perverse nationalism and historical wrongs into future narratives.

Pride—the other, reactive side of shame—is another core component of China's rise. Xi Jinping, then vice-president, told Robert Lawrence Kuhn in a March 2006 interview: "The Chinese people made great contributions to world civilisation and enjoyed long-term prosperity. Then we suffered over a century of national weakness, oppression and humiliation. So we have a deep self-motivation to build our country. Our commitment and determination is rooted in our historic and national pride."[43]

The fact that China is now doing in the political–economic–diplomatic sphere what was done to it militarily 150 years ago points to the way power encourages similar behaviour in nations. Currently, this transformative force of power is making China wreak havoc on the world. There seems to be a directly proportional relation between China's growth and its rate of exacting vengeance, currently as a regional power with aspirations to be a global hegemon. According to scholars, being a regional power with aspirations to become a global hegemon, China is unlikely to embrace universal values.[44] Therefore, the world must be cautious about China's growing power. Humiliation and its prevention remain the driving force behind China's bravado and the aggression, as evident in its actions on the Indian border and in the

South China Sea, and the sovereign support it lends to its commercial actors, such as Huawei, to penetrate global markets.

In particular, China's aggressive policy is directed towards countries that it considers to be on friendly terms with the US, including Japan, the Philippines and India. While economic interdependence has created an atmosphere of strained peace between India and China,[45] the latter remains aggressive in its posture. This is evident in its recent incursion into Doklam, a territory in Bhutan. It also supports the thesis that as China gets richer and more powerful, its attacks on India's interests intensify.[46] China and India have always been at loggerheads; however, the situation was exacerbated after India signed the Civil Nuclear Deal with the US. The deal also hyphenated China with Pakistan on the security front.[47]

Examining it through another lens, China's aggression against India could be a reaction to what Beijing perceives as the US' goal: to encircle China using alliances with Japan and India.[48] The US encirclement goes from Japan and South Korea on China's north-eastern side; down around China's eastern and south-eastern seaboards through Taiwan, the Philippines, Vietnam, Thailand, Singapore, Australia; and up to China's western frontier with India and Pakistan.[49] Thus, Beijing's anti-India encirclement is a pre-emptive strategy to prevent the US' encirclement of China. Using its economic strength as well as military force, China is co-opting surrounding countries into the Beijing narrative, the most brazen being the institutional subjugation of Pakistan. China sees as an affront India's refusal to submit and, in response, extends support to Pakistan, and through it, to the Pakistani state-sponsored terrorist outfits, which specifically target India. Apart from geography, legacy is clearly another motivation for Xi: "India's growing proximity to the USA, and an assertive and confident government in New Delhi, can be said to be political challenges for Xi

Jinping, whose desire is to create an image for himself larger than Mao and Deng within the country."[50]

Internally, China uses shame to drive a monolithic nationalism,[51] through its Belt and Road Initiative (BRI), the clamour for a "peaceful reunification with Taiwan," and holding back the iron hand on the legal aggression in Hong Kong. All three projects attempt to showcase Xi Jinping as a global statesman, bringing diverse geographies together into a singular China-dominant economic narrative. All three are driven by the propaganda of peace disseminated by the state-controlled media, but are predatory in their approach. The BRI attempts to push the China narrative against the US; Taiwan and Hong Kong, which have higher per capita incomes (2.5 times and 4.5 times, respectively) than mainland China's are part of the country's territorial predatory extensions and peaceful pretensions. However, all three are failing projects. Both Taiwan and Hong Kong are relentlessly resisting Chinese coercive actions. China's consensual nationalism works well with countries it can dominate politically, economically, ideologically or strategically, such as Pakistan, North Korea, Russia, some African nations, a few European nations such as Montenegro, whose public finances through a complex economic-legal model are shattered by a Chinese loan,[52] and Italy.

When China humiliates India or harms its interests regularly, almost as part of an obsessive state policy, they are actions of a powerful nation that is anchored in the weakness of humiliation. India can stand its own and return the favour diplomatically, as it did in two recent cases. First, when China was forced to sign off on declaring Masood Azhar as a global terrorist, after vetoing it thrice.[53] Second, when China unsuccessfully attempted to take India's abrogation of Article 370 to the United Nations Security Council (UNSC).[54] Militarily, India can stand its own, as the Doklam episode proved.

Most curious is China's support to Pakistan, despite the latter being the hub of global terror.[55] One wonders for how long Pakistan, a country that openly uses terror as a state policy against India, will continue to get China's support. This question assumes importance beyond India, as Xi has pretensions to be a global rule-maker. That is, to make rules that other countries will follow—not China. In Xi's race to reaching that goal, India stands as a moral, political and economic hurdle with support from most developed nations and strong economies. It is equally true that in the game-changing chessboard of international affairs, as nations dance to their national interests, leaving friendships or enmities aside, it is not known how long this support will last. India must not take this goodwill for granted; it must be constantly nurtured and nourished.

An alternative perspective to consider is the possibility that China's "Century of Humiliation" narrative is a strategic cloak to hide crimes committed by Chinese leaders and the state—both past offences and those that are happening today, including the repression of Uighurs in Xinjiang[56] and the ongoing citizens' struggle in Hong Kong.[57] In the past, China's propaganda machinery has whitewashed its historical atrocities. For example, the effective erasure (from both history and scholarship) of Mao Zedong's role in the peacetime death of millions of Chinese people.[58] In the ten years spanning the cultural revolution, "between 1.5 and 2 million people were killed, but many more lives were ruined through endless denunciations, false confessions, struggle meetings and persecution campaigns."[59] Mao weaponised food and tyrannised a nation with "at least 45 million people worked, starved or beaten to death."[60] So efficiently has the Chinese government managed to infiltrate the media and academia and push for omissions, that even academics have been forced to call out their own community: "The authors were so intent on proving inoffensive – even to the Chinese Communists – that they neglected to mention that Mao Zedong had

killed millions of his own people. The omission allowed them to write of the 'enthusiasm' of a billion people, while dismissing 40 years of tyranny as insufficient to judge a regime."[61] Closer to current times, the CPC has been doggedly attempting to whitewash the Tiananmen Square massacre (4 June 1989), in which 2,600 people were estimated to have been killed and 7,000 wounded.[62] Such brutal censorship within China has ensured that Chinese youth have little awareness of this massacre. Using a mix of market seduction for the world and political constriction within the country, China has, by and large, managed to reduce—if not remove—this taint from its domestic history. Fear perpetuates this censorship amongst the youth even today.[63]

The world needs to call out China's bluff on this false narrative and propaganda of yesterday that China has weaponised into a fine art to hide its serial tyrannical actions today.

## 5. BANS ON HUAWEI

Currently, India is on the fence about an outright ban on Huawei. In coming to a decision, India can reflect on what other nations are doing.

For example, Vietnam has rejected Huawei based on the actions of the Chinese state. The US$240-billion economy—substantially smaller than China's $14.2-trillion economy—cannot "risk their critical infrastructure just because they offer something cheaper than other companies."[64] Vietnam's ban has been driven as much by the state as by the people. According to the Pew Research Center's Global Indicators Database, only 10 percent of Vietnamese viewed China favourably in 2017 (down from 19 percent in 2015),[65] compared to 84 percent that view the US favourably (up from 78 percent).[66] Amongst other issues, China has created a standoff in the oil-producing waters off Vietnam's

coast, which fall within the latter's exclusive economic zone and where it has awarded oil concessions.[67] Territorial disputes, which Xi Jinping has turned into a weapon of shame and assault, has left Chinese companies with little moral capital in Vietnam.

The numbers in India are not very different: only 12 percent Indians had a favourable opinion of China in 2018, the lowest amongst the 27 countries ranked.[68] Essentially, the Chinese state—through Xi, in particular, and the CPC, in general—has become the biggest hurdle for Chinese companies. It has perhaps become difficult for Chinese companies, functioning under the benign eye of Xi's Chinese state, to globalise without carting within its structures the political ambitions of China. Especially when it comes to technologies or technology-driven critical infrastructure, the stakes have skyrocketed into the security domain.

Australia's case offers lessons for India and the rest of the world. On 19 August 2019, Australia's Foreign Investment Review Board chairman, David Irvine, made a speech in which he elegantly argued for keeping Chinese companies out of critical infrastructure sectors.[69] "Australia benefits from the openness of our foreign investment review framework. We will review foreign investment proposals to ensure they are not contrary to the national interest. By mitigating risks to the national interest, we protect the integrity of that open system," he said. "National security concerns" and policy equivalence with China remain the overriding feature of excluding Chinese firms from Australia's telecommunications sector. Again, China's NIL drives the reaction.

> "Many countries, like China, prohibit foreign ownership in key sectors or simply keep these assets under government ownership. In Australia, many assets are in private hands – including infrastructure, media and telecommunications

companies. Private ownership does not, however, absolve government of responsibility for ensuring Australia's critical infrastructure is secure and resilient – particularly in today's age of dependence on the cyber world.

These policies are an example of how the Australian Government places extra emphasis on some sectors of the economy, just as I understand the Chinese Government does in some sectors of its economy."[70]

On the world telecom map, the Huawei ban is a mixed bag. Other than Australia, countries that have banned Huawei include Vietnam, New Zealand, Japan, Taiwan and the US.[71] Together, they comprise one-third of the global GDP.[72] On the other hand, countries that have embraced Huawei include China, Russia,[73] Qatar, Saudi Arabia, the United Arab Emirates, South Africa,[74] Turkey,[75] Malaysia,[76] Nepal[77] and Germany.[78] Additionally, Bahrain, Kuwait and Oman are on their way.[79] Indonesia has kept its options open and has made no decision so far.[80] France, Italy and South Korea have shown no inclination to ban Huawei. Currently, the fence-sitters include Norway, Sweden, UK and India.

It is difficult to comment on what other nations or organisations should or shouldn't do. However, India cannot have an openly hostile foreign company operating within its boundaries and delivering critical infrastructure, especially one that insists on following China's laws.

This divergence in the geopolitics of 5G and its risks to big business and society are showing up in different ways. The Forum of Incident Response and Security Teams, comprising internet emergency response teams from 92 countries, 490 corporations, government bodies, universities and other institutions, has suspended Huawei's membership.[81] China is risky in terms of not only software or network

but also the hardware embeds. According to a *Bloomberg* report, Chinese spies used a tiny sabotage chip, the size of a pencil tip, to reach almost 30 US companies, including Amazon and Apple, by compromising America's technology supply chain.[82] Once Chinese companies entered the global supply chains of technological hardware, the risks turned into attacks. The report concludes that any hope that China will not allow politics to jeopardise its economics were dashed aground:

> "Over the decades, the security of the supply chain became an article of faith despite repeated warnings by Western officials. A belief formed that China was unlikely to jeopardise its position as workshop to the world by letting its spies meddle in its factories. That left the decision about where to build commercial systems resting largely on where capacity was greatest and cheapest. 'You end up with a classic Satan's bargain,' one former US official says. 'You can have less supply than you want and guarantee it's secure, or you can have the supply you need, but there will be risk. Every organisation has accepted the second proposition.'"

The role of the Chinese state in Chinese companies has grown under Xi Jinping. Using a mix of invisible incentives and penalties, the entwined structure of the state and the firm has turned Chinese companies into tools for information-collection, even when it comes to Chinese consumers in China. Thus, China has become what is without doubt an open surveillance state, a *Guardian* report notes:[83]

> "Meanwhile, China's three dominant internet companies, Baidu (a search engine), Alibaba (e-commerce) and Tencent (messaging and gaming), known collectively as the BAT, have all felt the government's wrath. In 2018, Tencent lost $200 billion in its market capitalisation after regulators stopped approving new online games, pushing the company out of the world's top 10

> companies ranked by their share market valuation. The rapid growth of the BAT companies and their dominance of the internet in China has given them an outsized economic status. But their political value is just as important, as they have become indispensable to China's surveillance state. With the mountain of data they generate, the BAT trinity are in effect turning into a real-time, efficient and privately run intelligence platform. In that respect, they are seen as ideal private companies. They both drive economic growth and also buttress the political system."

The questions that then arises is this: If being spied upon by China is acceptable to some countries, what makes it different for India? The answer lies in regional domination. China fears that if India is allowed to rise, it will lose its regional monopoly of hegemony in the Asian region. This is evident in China's opposition to India's membership to the Nuclear Suppliers Group[84] and to the UNSC. Beijing likely fears that if India and Japan are allowed entry, the US camp would strengthen.[85] To China, a rising India is an acute threat.[86] Driven by its own national interest, China is therefore doing its best to smother India's rise. At the same time, it is attempting to use India as a market to create an unsustainable trade surplus that stands at US$58 billion. While this surplus may contract in the short term, as the US–China relationship shifts to a new equilibrium,[87] the medium- to long-term goal of China to subdue India using economic benefits gained from it is unlikely to change.

Finally, in the context of Huawei (or any Chinese company), it would be a false equivalence to compare the response of other countries to India's. The risk that Huawei carts to Germany or Italy, for instance, are limited to data security. Rivalry, if any, is restricted to the efficiency of production and pricing. China does not stand to gain by disrupting Germany's critical infrastructure. In the case of India, however, the stakes

are substantially higher, given the India–China rivalry, in trade, foreign policy as well as national security. This is discussed in greater detail in Section 8.

## 6. INDIA–CHINA TRUST DEFICIT

In recent years, China's hostility towards India has become prominent, and the trust deficit between the two nations has grown. Attempting to drag the abrogation of Article 370 by Indian Parliament to the UNSC at the behest of Pakistan—in a case that will go down in diplomatic history as another instance of humiliation for China[88]—is only the latest in a series of its recent anti-India actions. China faced similar humiliation earlier, when it attempted to prevent Masood Azhar from being declared a global terrorist but gave up due to the fear of international humiliation and diplomatic isolation.[89]

The trust deficit cannot be filled by Indian actions alone. "China continues to be in occupation of a large tract of area in the Union Territories of Jammu and Kashmir, and Ladakh. It has illegally acquired Indian territories from PoK under so called China-Pakistan boundary agreement of 1963," said MEA spokesperson Raveesh Kumar, in response to China's unwarranted and incorrect statement that the scrapping of Article 370 challenges China's sovereignty. As long as China continues to see India as competition—economically and politically—India would be wise not to hand over its critical infrastructure to a Chinese firm.

China has set itself up for another humiliation in February 2020, when it plans to support Pakistan's terror infrastructure in the Financial Action Task Force plenary meeting.[90] By denouncing other members of the FATF, whose chair currently resides with China, it has already made its intentions clear.[91] Considering China's hostile actions from the

outside, it is only likely that this aggression will escalate once it enters India's strategic space through Huawei.

So far, China's attacks on India have only resulted in diplomatic ricochets, whereby China ends up humiliating itself. However, with each aggression, there is an increase in the trust deficit between the two nations. Under these circumstances, India does not stand to gain from China, and the latter cannot expect to feed off India's markets while harming its security and strategic interests. India will need to reimagine its relationship with China, argue Samir Saran and Akhil Deo: "It must recognise the long-term political threat from China, prepare to respond to Beijing's assertiveness in the medium term, and embrace China economically in the short term."[92]

Both countries need to end this trust deficit and reach a strategic-geopolitical equilibrium. Today, no major constituency in India has a favourable view of China.[93] In a democracy, where power comes from the vote of the people, this has serious implications for Huawei. India is bound by the constraint of following the rule of law, for instance, which an authoritarian China with a centralised leadership isn't. The Indian State—comprising the government, Parliament and the judiciary—must ensure that the strength of India's democracy is not diminished by the weight of its own institutions.

Given China's clear and consistent misbehaviour with India on all fronts—the border, support to Pakistan, trade, diplomacy, UNSC, NSG, dumping—India must work under the assumption that the Chinese state can potentially use Huawei's network to attack India from within. While business analysts might resist the rejection of Huawei based on financial indicators, the government must consider the strategic axiom clear to security analysts—that Huawei poses a clear and present threat to India.

## 7. THE POWER OF NATIONALISM

Security in the 5G space is not a play between security agencies alone. Underlying the actions of the government are three constituencies: companies, consumers and citizens. A rising political nationalism is influencing these constituencies and driving political choices. The telecommunications business needs the power of consumers to sustain itself. If a company decides to use Huawei equipment for its 5G network, and enough noise about its dangers is created, it would take just two days for consumers to shift to another operator.[94] Thus, even without the government officially banning the company, consumers can control the market using interoperability as a tool and nationalism as a force. The desire to retain customers—and through them, market value—will discourage the boards of directors of telecom firms from using Huawei equipment. Thus, even though Huawei's 5G equipment is cheaper than that of Ericsson and Nokia by around 20 percent,[95] the prospect of a tanking market will act as sufficient disincentive. Appeals and arguments by telecommunications lobbies around the increased costs of using alternative, non-Chinese 5G equipment[96] will have to be countered by the larger, no-compromises issue of national security.

The increased cost as a result of using non-Huawei equipment is a price that businesses, and through them consumers, must agree to pay in the interest of national security. Moreover, being a business with a long-gestation period, the premium now, amortised over the next two decades or so, will add up to very little in terms of the overall cost. For its part, the government can help by lowering 5G spectrum pricing. Instead of maximising auction revenues, for instance, it can embed security concerns into technical requirements and make economic allowances for effectively outsourcing security to commercial players, which will function under a rigorous regulatory umbrella. The commercial advantage pricing offers must be nullified by the security sweep.

"The future does not belong to globalists," said US President Donald Trump at the United Nations General Assembly in his 24 September 2019 speech.[97] "The future belongs to patriots. The future belongs to sovereign and independent nations, who protect their citizens…" He added, "If you want freedom, take pride in your country. If you want peace, love your nation."

Rhetorical as the words might sound, there is no denying the rise of nationalism across the world. Whether it is the US, Mexico, Turkey or Russia, there is a new surge of the nationalist spirit creating and driving new leaders. The globalists would like to devalue them by terming the leaders "strong men," even when they are operating within genuinely democratic systems but whose political appeal is around the idea of decisive leadership and nationalism.[98] Nationalism is here and, in the foreseeable future, likely to stay. Xi Jinping's aspirations for China as well as Prime Minister Narendra Modi's actions in India are driven by the same idea of nationalism.

In the middle of these conflicting nationalisms stands Huawei. Given the current nationalist political climate change, therefore, there is no room for lax policies or concessions for hegemonic bullies, if the sovereign state has to be protected. Toleration in trade deficits or cultural affairs is one thing; compromises on national security quite another. Being a technology that has deep and wide ramifications on the security of India, 5G will be questioned, its actions regulated. However, in case the government fails to do its part, consumer–investor citizens can build a user-driven wall, utilising the power of choice. The recent rise of nationalism has not been restricted to politics. Companies and traders, too, are putting their weight behind nationalism. The Solvent Extractors' Association of India, for instance, has asked its members to stop buying palm oil from Malaysia, following the latter's short-sighted criticism of India over the abrogation of Article 370. India is Malaysia's

third-largest export destination, and palm oil exports comprise 4.5 percent of its total exports to India. Thus, India's embargo on palm oil imports from Malaysia will hurt the Islamic nation's economy.[99]

The idea of India-first, like America-first or China-only, is the new global political narrative. International engagements at the UN are being increasingly replaced by bilateral talks and multilateral relationships: G20 (group of 20), as the board of directors overseeing the global economy; BIMSTEC (Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation), as a regional grouping; the Quadrilateral Security Dialogue (Quad); and the G2 (the US and China) meetings.

It has taken a long time for India to clearly define its India-first foreign-policy stance. In this context, any company that uses Chinese equipment for critical infrastructure will fall short of the nationalistic expectations from consumers and investors. Unless China's policies and actions show a visible shift towards India, Huawei will remain a technology pariah. Since the 5G technology has a far greater permeation, its consumer and investor recoil, riding a new nationalism, will be equally intense.

## 8. GEOGRAPHY: THE FINAL HURDLE

India's geographical proximity to China further adds to the former's security concerns. In the past, China has repeatedly wielded this against India. In 1962, it illegally occupied Aksai Chin. In March 1963, China coaxed Pakistan to hand over 5,180 square km of Indian territory in Shaksgam valley (Pakistan Occupied Kashmir)[100] in return for strategic support.[101] The 3,488-km long border that India shares with China,[102] parts of which are disputed, is "a classic study of great power rivalries, the perils of buffer states and the legacies of empires."[103] Since China has taken this rivalry beyond limits of tolerance, it has become a tipping point

for security-embedded engagements such as the entry of Chinese firms into India's critical infrastructure. This is not to say that the intrusions Chinese technology brings will not exist in equipment from other nations such as Finland or South Korea. However, India's geopolitical reality makes the threat from Chinese equipment significantly more dire.

India must, of course, continue its political engagement with China and attempt to get China to soften its aggressive stance. Discussions with scholars from China over the past 12 months have shown that Chinese intellectuals are conscious of India's concerns, be they China's encirclement of India, the China-Pakistan Economic Corridor that illegally passes through Indian territory, or the adversely high trade balance. While more leader-to-leader engagements with China are underway, India must temper expectations from informal meets as those that happened in Wuhan in 2018,[104] Mamallapuram in 2019[105] and the third one planned for 2020 in China.[106]

For its part, China must understand that the diminishing marginal returns from hostilities against India have set in. For instance, threatening India with reverse sanctions if it blocks Huawei[107] will not be helpful. Instead, China must actively attempt to fix its relationship with India. Until ties are mended on the security front, the best India can offer is a delay in the launch of 5G services, allowing China time to reform and rework its legal structures.

## 9. 5G IN INDIA: SIX POLICY CONTEXTS

For a US$2.7-trillion economy that hopes to become a US$5-trillion economy in five years and US$10-trillion in 13 years, India must now look inwards and keep domestic needs in mind. The primary concern in the 5G roll-out is national security, and according to V. Kamakoti, professor at IIT Madras and member of the National Security Advisory

Board,[108] India cannot afford to take chances in this matter. Thus, India must strike a balance between keeping up with technology and its benefits and protecting India's national interest. While there are no answers for now, the following six contexts merit a deeper debate and act as policy pointers as India drafts its 5G policy.

## 1. Indigenisation

Despite all calls and support for nationalism, in the globalised 21st century, the word indigenisation may stand out as being out of sync. But in the sub-world of security, India must not forget that it has managed to deliver high-technology products indigenously. From space research through Indian Space Research Organisation (ISRO) to going nuclear through the Atomic Energy Commission, India has been able to develop and deliver high-technology. Once the political will is clear, the development of future telecommunications technologies such as 5G onwards may not be such a difficult task. What is necessary is to develop India-specific hardware and software. India has to reinvent the equipment that exists.

Already, trials are underway. The 5G TestBed Project is led by IIT Madras and CEWiT with support from the Ministry of Communication and Information Technology. Amongst other things, they are working on developing some "revolutionary concepts" such as millimetre wave communication, massive MIMO (multiple-input multiple-output), dense networks and wireless solutions for Indian markets in conjunction with the industry.[109] A similar testbed project at IIT Madras, called "Indigenous 5G TestBed: Building an End-to-End 5G Test Bed in India," is expected to be completed by March 2021.[110]

Indigenisation will help India to avoid getting caught between a US-influenced ecosystem and a China-determined ecosystem, and allow it

to procure components individually. India can aim at creating an open and non-allied ecosystem, like Linux for telecommunications. In the geopolitics of 5G standards, India must make its requirements count; India's geography, for instance, is diffused across villages with little infrastructure. The standards are currently being dominated and influenced by American and Chinese firms.[111] Voices of 'the 5G have-nots' must be heard and served. Along with indigenisation, India must tailor the global 5G standards to fit its requirements. Further, while developing a system, India must inject flexibilities into the system such that it can incorporate further innovations and be future-ready.

## 2. Government in Business

The Indian government has had many failings in the business sector: the abysmal performance of Air India on all parameters; the imploding BSNL and MTNL; the wasteful recapitalisation of public-sector banks, whose market value is less than the money invested; the unaccountability of consumer-facing staff at all public-sector enterprises. However, the security space is unique, and the government's role in it must be examined through different lenses.

The government must rethink its commercial enterprises and, using a mix of capital investments and professional freedom, create several ISRO-like organisations. Another strategy would be to develop PPP models, pooling in the expertise of both the private and public sector to create a 5G infrastructure. While this infrastructure may not be cutting edge or the most cost-effective, it would be the most secure and with the highest levels of control. Since the government refused to sell or shut down BSNL and MTNL, instead deciding to merge them, keeping spectrum allocation and retirements in mind,[112] this merged entity can become a pilot for experimenting with 5G equipment.

## 3. Government as Enabler

While building another ISRO-like organisation may be difficult, creating an enabling mechanism is not. India must create a three-part ecosystem comprising policy, knowledge and execution. The first component of this ecosystem requires the government to adapt to the changing needs of the nation. The second component is related to private enterprises and individuals, where the government must step aside and give greater operating flexibility in research labs, on factory floors, around labour mobility. Additionally, it must create policy islands of freedom—smart industrial townships, for instance—in cities, with education and healthcare facilities for attracting global talent. The final component is allocating greater freedom to universities and embedding accountability in the end product or the processes. That is, providing the money and flexibility needed to recruit talented individuals as faculty or researchers, (from anywhere and at any salary in government-funded universities, and financial and operational freedom in courseware design or fee structures in private universities.

Institutes of eminence, both private and public, have already started implementing this model.[113] Between the three actors—the private sector as the driver, the universities as technology creators and researchers, and the government as enabler—and with sharp targets in place, the model has the potential to yield great results. The three must work as a team, albeit each with its own sets of incentives, to contribute to an independent India-focused ecosystem.

## 4. Technological Nationalism

Part of China's growth can be attributed to what is termed as "technonationalism," wherein the country has demanded the transfer of technology from foreign firms. China has gone about it in an organised

manner, using what Katherine Koleski and Nargiza Salidjanova call "China's Industrial Policy Toolbox."[114] This toolbox includes 10 key instruments that merge economic growth and strategic control with hegemonic aspirations and nationalism, namely, localisation targets, state funding, government-funded research and development, government procurement, creating China-specific technology standards, regulatory hurdles for non-Chinese firms, restrictions on foreign investments, financing private Chinese companies to acquire foreign technology, and industrial espionage. While such a policy direction may be difficult for a democratic India to demand and obtain, the model must be studied before negotiating with China on such policy asymmetries.

Japan has used military technonationalism in the past, but it has now shifted to commercial technonationalism. Japan's military and industrial strategies have been built on a fusion of industrial, technology and national-security policies.[115] For both Japan and China, the three pillars of technonationalism were indigenisation, diffusion and nurturance.[116] Finally, under its "Innovation Union Policy," there seems to be a resurgence of technonationalism in the European Union, through protectionist policies and actions in support of high-tech industries.[117]

On the other hand, technonationalism in the 21st century may not entirely reflect its preceding avatars. Talking about the US and China falling into the "Thucydides Trap" (established and rising powers inevitably clashing to the point of military conflict), Nathan Gardels argues that what could most likely "trip this trap is an unyielding technonationalism that is emerging in both China and the United States."[118] This technonationalism has war-like tendencies. "What we are facing is not an ideological Cold War, or even a trade war, but in fact a tech war—that is, a war for control over technological standards and the

commercial spoils that go with that," argues Nils Gilman.[119] Situate this US–China argument in India–China context, and they apply with equal strength.

If a rising nationalism is taking the space left by a receding globalisation, indigenisation is clearly its transacting currency. In securing its critical infrastructure, India must attempt to move in this direction.

### 5. No Rush

Examining closely what 5G technology can deliver—smart cities and driverless cars, for instance—one finds that India is not ready. India's current physical infrastructure is incapable of handling such technological and sociological jumps in the way it lives and how its society functions. Therefore, India need not—and indeed, *should* not—rush to deliver 5G to its citizens. For best results, the 5G revolution must be preceded by a physical revolution.

Further, since new technologies take time to be perfected, India can turn its apparent weakness into a strength. Joining the 5G race later in the game will ensure that the technology has stabilised. In the interim, India can expect a data-protection law to be introduced in Parliament during the Budget session, as Law Minister Ravi Shankar Prasad has declared.[120] This law will mandate that Indian data be localised within its borders, which will prevent the data from flowing out to the West or (if India allows Huawei in) to China.

A recent Supreme Court judgement has ruled in favour of the government (against the private sector) on the definition of adjusted gross revenue,[121] putting the private sector under financial pressure. Consequently, two out of the three largest players may not be ready to bid

for the spectrum needed to deliver 5G. During the consultative process, therefore, the auction of 5G spectrum could be delayed. Thus, although India may lag by a few years on delivering 5G infrastructure, there will be no major loss to the nation. On the contrary, the delay will allow India the time to develop the infrastructure necessary for effectively using 5G.

### 6. Huawei's Function

Despite the many concerns surrounding the company, Huawei could serve an important function. The inexpensive equipment it provides can be used to pull down the prices of other companies. According to senior executives from telecommunications firms, had it not been for Huawei, the benchmark prices for future equipment purchases from other vendors would have begun at a much higher level. Those companies, while being more acceptable from a security perspective, would have extracted their rents through a less-competitive business environment. Lack of competition would also have facilitated product complacency and pricing dominance. Thus, Huawei can be seen as a pricing watchdog, more efficient than any regulator or government in the commercial space.

## 10. CONCLUSION AND RESEARCH DIRECTIONS

It is clear that there should be no Chinese company operating in India's critical infrastructure. This is applicable not just to Huawei in telecommunications but to all Chinese companies across industries. Banning Huawei is only the first step, and other Chinese companies operating in key sectors will soon follow suit.

China has made huge investments in Pakistan's terror against India and repeatedly attempted to smother India's aspirations in international forums. It has spent huge diplomatic capital in putting India down.

China has dragged the Kashmir issue to the UNSC, albeit failing miserably, even as it crushes its own citizens in Buddhist-dominated Tibet, Uyghur-Muslim-dominated Xinjiang, global citizens in Hong Kong, and the Taiwanese in its backyards. India's patience with China's ruthless, needless and wasteful aggression has now run its course. Until China shows a visible and verifiable change of intent, allowing Chinese firms in India's critical infrastructure would be acting against India's national interest and inviting political peril, particularly in the context of nationalism. Private firms, too, stand to lose consumers and business by engaging with Chinese companies. Unless Xi Jinping mends fences, New Delhi must continue to frame policies assuming the worst about Beijing's intentions.[122] Beijing cannot expect economic returns from India without making commensurate investments in building strategic ties. To rephrase, China has to climb its way up the trust vanguards of India before it enters the trust vaults of India.

This paper has laid out evidence and arguments that come together to argue that in its current form, Huawei must not be allowed into India's telecommunications sector. This we have done by examining the uniquely transformative 5G technology and its impact on society, how the global leader Huawei is well-placed to deliver 5G but has the wrong citizenship. This paper also studies how that citizenship is driven by an aggressive China with laws that make it binding on Huawei to collect and transmit intelligence to its home country. Driven by shame, China has weaponised shame against the world, and India in particular. Further, India will not be an outlier if it bans Huawei. Even if is, the focused attack on India combined with a long border and overt and covert support to terror from Pakistan makes it incumbent to prevent such a critical infrastructure from being handed to a Chinese firm. In India's favour is a rising nationalism under which not merely companies but also consumers and investors will shun any operator that will use

Huawei. Finally, this paper highlighted six policy contexts within which policymakers can debate this issue.

Looking ahead, India-focused researchers may study how companies that have legal bindings from a nation that is openly hostile to India will behave when building and benefitting from delivering critical infrastructure such as power generation and distribution, ports, airports, railways, and financial services in India. As India becomes a larger economy and its disparity with China reduces, new opportunities will show up. With every trillion-dollar increase in India's GDP, the economic relationship with China and the texture of accompanying conversations between the two countries will change. How this will impact the security and strategic relationship will open out new tributaries of research. Finally, over the next few years, perhaps even the Chinese will tire of Xi's aggression. Will that lead to a China that is more democratic, with greater adherence to the rule of law and more friendly towards India? Or will it become a more destructive hegemon? Within that, how India balances its geopolitical, commercial and strategic interests will be continuing areas of study.

Outside the Indian context, this paper paves the way for research around a singular but expanding question: How does foreign policy influence globalisation at the economic and technological level? In other words, in an age when corporations are transnational, regulation is local, products breach through inequalities, and services are united by a common aspiration, how do sovereigns deal with each other while delivering critical infrastructure? These questions will address tense foreign-policy relationships across the world across geographies—Russia's gas exports to Europe and China, China's 5G footprint, China's BRI across several countries in Asia and Europe, Germany's export of industrial robots, the US' AI technologies.

Read together, the underlying theme in all these research streams is one that will dominate the 21st century: globalisation of technologies on the one side, and regulations and citizen protections on the other. Of particular interest will be two specific areas. One, how foreign policies of nations adapt to a global world unified by corporations, products and services in the areas of security, privacy and intrusions. And two, how domestic policies react to a technologically globalised world within the paradigm of rising nationalism.

## ENDNOTES

1. Robert L. Slayer, "U.S. Policy on 5G Technology, Foreign Press Centers Briefing," 28 August 2019, accessed 25 October 2019, https://www.state.gov/US-Policy-On-5g-Technology.

2. Firooz B. Saghezchi, Jonathan Rodriguez, Shahid Mumtaz, Ayman Radwan, William C. Y. Lee, Bo Ai, Mohammad Tauhidul Islam, Selim Akl4 and Abd Elhamid M. Taha, "Drivers for 5G: The 'Pervasive Connected World'" in *Fundamentals of 5G Mobile Networks*, ed(John Wiley & Sons, Ltd., 2015), 3-4, accessed 19 September 2019, https://5g.itrc.ac.ir/sites/default/files//Fundamentals%20of%205G%20Mobile%20Networks-Wiley%20%282015%29.pdf.

3. A UN agency for information and communication technologies whose members include 193 states and 900 companies, universities, and international and regional organisations.

4. ITU-R Recommendation M.2083-0, Cited in "Setting the Scene for 5G: Opportunities & Challenges," International Telecommunication Union, 2018.

5. "Study Paper on 5G-Key Capabilities & Applications," FN Division, Telecommunication Engineering Centre, Department of Telecommunications, Ministry of Communications, Government of India, March 2019, accessed 28 November 2019, http://tec.gov.in/pdf/Studypaper/5G%20Study%20Paper-approved%20by%20Sr%20DDG.pdf.

6. Ibid.

7. D. Minoli and B. Occhiogrosso, "IoT Applications to Smart Campuses and a Case Study," EAI Endorsed Transactions on Smart Cities, DVI Communications, European Alliance for Innovation, 19 December 2017, accessed 31 October 2019, https://eudl.eu/pdf/10.4108/eai.19-12-2017.153483.

8. Ibid.

9. Alex Kliment and Ari Winkleman, "Graphic Truth: Huawei's Supply Chain Bind," *Gzero*, 12 June 2019, accessed 22 October 2019, https://www.gzeromedia.com/graphic-truth-huaweis-supply-chain-bind.

10. "Huawei to develop radars for self-driving cars, top executive says," *Reuters*, 22 October 2019, accessed 25 October 2019, https://in.reuters.com/article/us-huawei-tech-autonomous/huawei-to-develop-radars-for-self-driving-cars-top-executive-says-idINKBN1X11HU.

11. Emeka Obiodu and Mark Giles, "The 5G era: Age of boundless connectivity and intelligent automation," GSMA, 2017, accessed 26 September 2019, https://www.gsmaintelligence.com/research/?file=0efdd9e7b6eb1c4ad9aa5d4c0c971e62&download.

12. "Road to 5G: Introduction and Migration," GSMA, April 2018, accessed 31 October 2019, https://www.gsma.com/futurenetworks/wp-content/uploads/2018/04/Road-to-5G-Introduction-and-Migration_FINAL.pdf.

13. "Huawei Facts," Q&A, Company Website of Huawei, accessed 28 November 2019, https://www.huawei.com/en/facts.

14. "U.S. intelligence says Huawei funded by Chinese state security: report," *Reuters*, 20 April 2019, accessed 15 September 2019, https://www.reuters.com/article/us-usa-trade-china-huawei-idUSKCN1RW03D.

15. Dan Strumpf and Patricia Kowsmann, "U.S. Prosecutors Probe Huawei on New Allegations of Technology Theft," 29 August 2019, *The Wall Street Journal*, accessed 15 September 2019, https://www.wsj.com/articles/u-s-prosecutors-probe-huawei-on-new-allegations-of-technology-theft-11567102622.

16. Zak Doffman, "CIA Claims It Has Proof Huawei Has Been Funded By China's Military And Intelligence," *Forbes*, 20 April 2019, accessed 15 September 2019, https://www.forbes.com/sites/zakdoffman/2019/04/20/cia-offers-proof-huawei-has-been-funded-by-chinas-military-and-intelligence/#275876857208.

17. "Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice," Department of Justice, Office of Public Affairs, 28 January 2019, accessed 15 September 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade.

18. "Addition of Entities to the Entity List," Federal Register, *The Daily Journal of the United States Government*, Bureau of Industry and Security, Commerce, 21 May 2019, accessed 15 September 2019, https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list.

19. Iris Deng, "Huawei's 5G gear seen as a bargain in many European capitals even though Polish arrest lifts security stakes," *South China Morning Post*, 14 January 2019, accessed 28 November 2019, https://www.scmp.com/tech/big-tech/article/2182005/huaweis-5g-gear-seen-bargain-many-european-capitals-even-though-polish.

20. Keith Johnson and Elias Groll, "The Improbable Rise of Huawei," *Foreign Policy*, 3 April 2019, accessed 28 November 2019, https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/.

21. Michael Grothaus, "Huawei just unveiled HarmonyOS, its answer to Android—and Trump," *Fast Company*, 9 August 2019, accessed 16 September 2019, https://www.fastcompany.com/90388251/huawei-just-unveiled-harmonyos-its-answer-to-android-and-trump.

22. "Annual report of Huawei Investment & Holding Co., Ltd.,"

Company website of Huawei, accessed 2 December 2019, https://www.huawei.com/en/download?rid={762E723A-BAF2-48C3-904A-8B0149043200}.

23. Li Tao, "Huawei wins half of China Mobile's 5G network contracts while Ericsson picks up a third," *South China Morning Post*, 17 June 2019, accessed 16 September 2019, https://www.scmp.com/tech/big-tech/article/3014766/china-mobile-awards-half-its-5g-network-contracts-huawei-while.

24. PTI, "China rolls out 5G telecom services," *The Economic Times*, 1 November 2019, accessed 1 November 2019, https://economictimes.indiatimes.com/news/international/business/china-rolls-out-5g-telecom-services/articleshow/71851743.cms.

25. "Huawei obtains 46 commercial 5G contracts in 30 countries," *Xinhua*, 6 June 2019, accessed 16 September 2019, http://www.xinhuanet.com/english/2019-06/06/c_138122365.htm.

26. "Huawei: Work Together to Bring the Best 5G into Reality," Huawei company website, 24 June 2019, accessed 16 September 2019, https://www.huawei.com/en/press-events/news/2019/6/11th-huawei-user-group-meeting-wuzhen.

27. Lisa Eadicicco, "Huawei, the Chinese tech giant embroiled in controversy, just overtook Apple to become the second largest smartphone maker," *Business Insider*, 4 May 2019, accessed 16 September 2019, https://www.businessinsider.in/Huawei-the-Chinese-tech-giant-embroiled-in-controversy-just-overtook-Apple-to-become-the-second-largest-smartphone-maker/articleshow/69169120.cms.

28. Keith Johnson and Elias Groll, "The Improbable Rise of Huawei," *Foreign Policy*, 3 April 2019, accessed 16 September 2019, https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-

huawei-5g-global-network-china/.

29. Iain Morris, "For UK 5G Users, the Only Way Is Huawei," *Light Reading*, 24 June 2019, accessed 16 September 2019, https://www.lightreading.com/mobile/5g/for-uk-5g-users-the-only-way-is-huawei/d/d-id/752339.

30. "China's Huawei signs deal to develop 5G network in Russia," *The Guardian*, 6 June 2019, accessed 16 September 2019, https://www.theguardian.com/technology/2019/jun/06/chinas-huawei-signs-deal-to-develop-5g-network-in-russia.

31. Li Tao, "Nearly 60 per cent of Huawei's 50 5G contracts are from Europe," *South China Morning Post*, 19 July 2019, accessed 16 September 2019, https://www.scmp.com/tech/big-tech/article/3019248/nearly-60-huaweis-50-5g-contracts-are-europe.

32. Douglas B. Fuller, *Paper Tigers, Hidden Dragons: Firms and the Political Economy of China's Technological Development* (Oxford University Press, 2016) 82-83.

33. Kadri Kaska, Henrik Beckvard and Tomas Minarik, "Huawei, 5G and China as a Security Threat," The NATO Cooperative Cyber Defence Centre of Excellence, 2019, accessed 16 September 2019, https://ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf.

34. Ibid.

35. "A Transactional Risk Profile of Huawei," RWR Advisory Group, 13 February 2018, accessed 16 September 2019, https://www.rwradvisory.com/wp-content/uploads/2018/04/RWR-Huawei-Risk-Report-2-13-2018.pdf.

36. Christopher Ashley Ford, "Huawei and its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications," US

Department of State, 11 September 2019, accessed 2 December 2019, https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/.

37. "National Intelligence Law of the P.R.C. (2017)," China Law Translate, 27 June 2017, accessed 16 September 2019, https://www.chinalawtranslate.com/-NNSºNlqQŒTýVýV¶[Å`¥bÕl/?lang=en.

38. Carolina Dacko and Lucas Jonsson, "Applicability of Chinese National Intelligence Law to Chinese and non-Chinese Entities," *Mannheimer Swartling*, January 2019, accessed 22 October 2019, https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf.

39. Huawei Facts, Huawei website, accessed 1 November 2019, https://www.huawei.com/en/facts.

40. Ibid.

41. Louise Lucas, "China government assigns officials to companies including Alibaba," *Financial Times*, 23 September 2019, accessed 22 October 2019, https://www.ft.com/content/055a1864-ddd3-11e9-b112-9624ec9edc59.

42. Robert Lawrence Kuhn, *How China's Leaders Think: The Inside Story of China's Reform and What This Means for the Future* (Asia: John Wiley & Sons, 2010), http://www.urbanlab.org/articles/China/state%20and%20power/Kuhn%202010%20-%20how%20China%27s%20leaders%20think.pdf.

43. Ibid, Kuhn.

44. "How the West got China wrong: Decades of optimism about China's rise have been discarded," *The Economist*, 1 March 2018, accessed 15 September 2019, https://www.economist.com/briefing/2018/03/

01/decades-of-optimism-about-chinas-rise-have-been-discarded.

45. Albina Muratbekova, "The Sino-Indian border issue as a factor for the development of bilateral relations," *Asian Journal of Comparative Politics*, No. 1 (2018): 3–12, accessed 15 September 2019, https://journals.sagepub.com/doi/pdf/10.1177/2057891117690453.

46. Manoj Joshi, "Doklam: To Start at the Very Beginning," Observer Research Foundation, August 2017, accessed 15 September 2019, http://cf.orfonline.org/wp-content/uploads/2017/08/ORF_SpecialReport_40_Doklam.pdf.

47. Mehmood Hussain, "Impact of India-United States Civil Nuclear Deal on China-Pakistan Strategic Partnership," *Journal of South Asian Studies*, 2017.

48. R.L. Kuhn, op. cit.

49. David Lai, "US-China Relations: A New Start?" in *The People's Liberation Army and China in Transition*, ed. Stephen J. Flanagan and Michael E. Marti (Institute for National Strategic Studies, National Defense University, August 2003), accessed 13 September 2019, https://apps.dtic.mil/dtic/tr/fulltext/u2/a430961.pdf.

50. A.K. Bardalai, "Doklam and the Indo-China Boundary, *Journal of Defence Studies*," 12 no. 1 (January-March 2018): 5-13, accessed 13 September 2019, http://idsa.in/jds/jds-12-1-2018-doklam-indo-china-boundary.

51. Robert D. Weatherley and Qiang Zhang, "History and Legitimacy in Contemporary China Towards Competing Nationalisms," in *Religion and Nationalism in Chinese Societies*, ed. Cheng-tian Kuo (Amsterdam University Press, 2017), accessed 13 September 2019, https://www.jstor.org/stable/j.ctt1zkjzkd.9.

52. Noah Barkin and Aleksandar Vasovic, "Chinese 'highway to nowhere' haunts Montenegro," *Reuters*, 16 July 2018, accessed 13 September 2019, https://www.reuters.com/article/us-china-silkroad-europe-montenegro-insi/chinese-highway-to-nowhere-haunts-montenegro-idUSKBN1K60QX.

53. Gautam Chikermane, "4 faultlines in Masood Azhar's UN terrorist listing," Observer Research Foundation, 2 May 2019, accessed 13 September 2019, https://www.orfonline.org/expert-speak/4-faultlines-masood-azhar-un-terrorist-listing-50454/.

54. Gautam Chikermane, "From Balakot to Article 370, 2019 is becoming the year of India's rajasic transformation," Observer Research Foundation, 21 August 2019, accessed 13 September 2019, https://www.orfonline.org/expert-speak/from-balakot-to-article-370-2019-is-becoming-the-year-of-indias-rajasic-transformation-54625/.

55. Vanda Felbab-Brown, "Why Pakistan supports terrorist groups, and why the US finds it so hard to induce change," *The Brookings Institution*, 5 January 2018, accessed 28 November 2019, https://www.brookings.edu/blog/order-from-chaos/2018/01/05/why-pakistan-supports-terrorist-groups-and-why-the-us-finds-it-so-hard-to-induce-change/.

56. Lindsay Maizland, "China's Repression of Uighurs in Xinjiang," Council on Foreign Relations, 9 October 2019, accessed 28 October 2019, https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang.

57. Bethany Allen-Ebrahimian, "How China's repression playbook backfired in Hong Kong," *Vox Media*, 29 August 2019, accessed 28 October 2019, https://www.vox.com/world/2019/8/29/20835183/hong-kong-protests-china-repression-tiananmen-square-beijing-response.

58. Jon Halliday and Jung Chang, *Mao: the Unknown Story* (Vintage Books, 2007).

59. Frank Dikotter, *The Cultural Revolution: A People's History, 1962-1976* (Bloomsbury, 2017).

60. Ibid.

61. James Wunsch, "The Burden of History," *The Phi Delta Kappan*, 75, no. 6 (February 1994): 492-493, Phi Delta Kappa International, accessed 28 October 2019, https://www.jstor.org/stable/20405146.

62. M.E. Sarotte, "China's Fear of Contagion: Tiananmen Square and the Power of the European Example," *International Security*, 37, no. 2 (FALL 2012): 156-182, The MIT Press, accessed 28 October 2019, https://www.jstor.org/stable/23280417.

63. Bill Birtles, "Tiananmen Square 30th anniversary: How China erased iconic 'tank man' image for young people," *ABC News*, 4 June 2019, accessed 28 October 2019, https://www.abc.net.au/news/2019-06-04/tiananmen-30th-anniversary-young-people-dont-know-tank-man/11152324.

64. John Boudreau and Nguyen Dieu Tu Uyen, "Cybersecurity: Vietnam Prefers Its Mobile Networks to Be Free of Huawei," *Bloomberg*, 26 August 2019, accessed 16 September 2019, https://www.bloomberg.com/news/articles/2019-08-26/vietnam-prefers-its-mobile-networks-to-be-free-of-huawei?srnd=premium-asia.

65. "Opinion of China: Do you have a favorable or unfavorable view of China?," Global Indicators Database, Pew Research Center, accessed 16 September 2019, https://www.pewresearch.org/global/database/indicator/24/country/vn.

66. "Opinion of the United States: Do you have a favorable or unfavorable

view of China?," Global Indicators Database, Pew Research Center, accessed 16 September 2019 https://www.pewresearch.org/global/database/indicator/1/country/vn.

67. James Pearson and Khanh Vu, Vietnam, "China embroiled in South China Sea standoff," *Reuters*, 17 July 2019, accessed 16 September 2019, https://www.reuters.com/article/us-vietnam-china-southchinasea/vietnam-china-embroiled-in-south-china-sea-standoff-idUSKCN1UC0MX.

68. "Opinion of China, Do you have a favorable or unfavorable view of China?," Global Indicators Database, Pew Research Center, accessed 16 September 2019, https://www.pewresearch.org/global/database/indicator/24.

69. "Address by Mr David Irvine AO, FIRB Chair to the Australia-China Business Council," Foreign Investment Review Board, Australian Government, 19 August 2019, accessed 16 September 2019, http://firb.gov.au/about-firb/news/address-mr-david-irvine-ao-firb-chair-australia-china-business-council.

70. Ibid.

71. Katharina Buchholz, "Which countries have banned Huawei?," *Statista*, 19 August 2019, accessed 16 September 2019, https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/.

72. Ibid.

73. Zak Doffman, "Huawei Just Launched 5G In Russia With Putin's Support: 'Hello Splinternet'," *Forbes*, 1 September 2019, accessed 2 December 2019, https://www.forbes.com/sites/zakdoffman/2019/09/01/hello-splinternet-huawei-deploys-5g-in-russia-with-putins-support/#7b03be2f199d.

74. "Rain and Huawei launch South Africa's first commercial 5G network," *BusinessTech*, 26 February 2019, accessed 26 September 2019, https://businesstech.co.za/news/mobile/301934/rain-and-huawei-launch-south-africas-first-commercial-5g-network/.

75. "Mobile operator Turkcell ready to launch 5G, says CEO," *Hurriyet Daily News*, 12 December 2018, accessed 26 September 2019, http://www.hurriyetdailynews.com/mobile-operator-turkcell-ready-to-launch-5g-says-ceo-139675.

76. Krishna N. Das, "Malaysia's 5G plan a potential boon for China's Huawei," *Reuters*, 24 September 2019, accessed 26 September 2019, https://www.reuters.com/article/us-telecoms-5g-malaysia/malaysias-5g-plan-a-potential-boon-for-chinas-huawei-idUSKBN1W90RD.

77. Benjamin Parkin, "Nepal's only billionaire enlists Huawei to transform country's telecoms," *Financial Times*, 4 September 2019, accessed 26 September 2019, https://www.ft.com/content/8d181320-ca12-11e9-a1f4-3669401ba76f.

78. Andreas Rinke, Douglas Busvine, "New German rules leave 5G telecoms door open to Huawei," *Reuters*, 14 October 2019, accessed 26 October 2019, https://www.reuters.com/article/us-germany-telecoms-5g-idUSKBN1WT110.

79. John Calabrese, "The Huawei Wars and the 5G Revolution in the Gulf, Middle East Institute," 30 July 2019, accessed 26 September 2019, https://www.mei.edu/publications/huawei-wars-and-5g-revolution-gulf#_ftnref1.

80. Fathiya Dahrul, "Southeast Asia's Top Phone Carrier Still Open to Huawei 5G," *BloombergQuint*, 26 September 2019, accessed 26 September 2019, https://www.bloombergquint.com/global-economics/southeast-asia-s-largest-carrier-leaves-door-open-for-huawei-5g.

81. "Statement regarding Huawei's suspension from the Forum of Incident Response and Security Teams (FIRST)," Forum of Incident Response and Security Teams, 18 September 2019, accessed 22 October 2019, https://www.first.org/_/downloads/first-press-release-20190918.pdf.

82. Jordan Robertson and Michael Riley, "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies," *Bloomberg*, 4 October 2018, accessed 16 September 2019, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

83. Richard McGregor, "How the state runs business in China," *The Guardian*, 25 July 2019, accessed 16 September 2019, https://www.theguardian.com/world/2019/jul/25/china-business-xi-jinping-communist-party-state-private-enterprise-huawei.

84. Press Trust of India, "China rules out India's entry into NSG without 'consensus' on allowing non-NPT countries," *The Economic Times*, 21 June 2019, accessed 16 September 2019, https://economictimes.indiatimes.com/news/defence/china-rules-out-indias-entry-into-nsg-without-consensus-on-allowing-non-npt-countries/articleshow/69893448.cms.

85. J. Mohan Malik, "Security Council Reform: China Signals Its Veto," *World Policy Journal*, 22, no. 1 (Spring, 2005): 19-29, Duke University Press, accessed 28 October 2019, https://www.jstor.org/stable/40209946.

86. Hemant Adlakha, "China Is Starting to See India as a Major Threat," *The Diplomat*, 11 January 2018, accessed 17 September 2019, https://thediplomat.com/2018/01/china-is-starting-to-see-india-as-a-major-threat/.

87. Kirtika Suneja, "India may trade places with US to ship items to

China," *The Economic Times*, 17 June 2019, accessed 17 September 2019, https://economictimes.indiatimes.com/news/economy/foreign-trade/india-may-trade-places-with-us-to-ship-items-to-china/articleshow/69818455.cms.

88. Elizabeth Roche, "At UNSC, China and Pakistan fail to censure India over Article 370," *Mint*, 17 August 2019, accessed 17 September 2019, https://www.livemint.com/news/india/at-unsc-china-and-pakistan-fail-to-censure-india-over-article-370-1565978919225.html.

89. Rupakjyoti Borah, "Will US reward China for 'sacrificing' Pakistan terrorist Masood Azhar?," *South China Morning Post*, 8 May 2019, accessed 17 September 2019, https://www.scmp.com/week-asia/opinion/article/3009415/will-us-reward-china-sacrificing-pakistani-terrorist-masood-azhar.

90. "Outcomes FATF Plenary, 16-18 October 2019," Financial Action Task Force, 18 October 2019, accessed 22 October 2019, https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-october-2019.html.

91. "China denounces FATF members for pursuing political agenda against Pakistan," *The Express Tribune*, 29 October 2019, accessed 31 October 2019, https://tribune.com.pk/story/2089153/3-china-denounces-fatf-members-pursuing-political-agenda-pakistan/.

92. Samir Saran and Akhil Deo, *Pax Sinica*: *Implications for the Indian Dawn* (Rupa Publications, 2019), pp 86.

93. Harsh V. Pant, "New Delhi's options in the face of Beijing's stance on Kashmir," *Mint*, 22 August 2019, accessed 17 September 2019, https://www.livemint.com/opinion/online-views/opinion-new-delhi-s-options-in-the-face-of-beijing-s-stance-on-kashmir-1566493182678.html.

94. Rahul Sethi, "Porting your mobile number gets easier, will take just

two days," *India Today*, 15 December 2018, accessed 29 November 2019, https://www.indiatoday.in/technology/news/story/porting-your-mobile-number-gets-easier-will-take-just-two-days-1410265-2018-12-15.

95. "Huawei 5G Technology Is 20% Cheaper Than Rivals And In The Same Time – Superior To Them Too," *Alertify*, 10 November 2019, accessed 29 November 2019, https://alertify.eu/huawei-5g-technology-is-20-cheaper-than-rivals-and-in-the-same-time-superior-to-them-too/.

96. Gwénaëlle Barzic, "Europe's 5G to cost $62 billion more if Chinese vendors banned: telcos," *Reuters*, 7 June 2019, accessed 28 October 2019, https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3.

97. Donald Trump (realDonaldTrump), "The future does not belong to globalists. The future belongs to patriots. #UNGA," *Twitter*, 24 September 2019, accessed 25 September 2019, https://twitter.com/WhiteHouse/status/1176534392556183554?s=20.

98. "Gideon Rachman, Trump, Putin, Xi and the cult of the strongman leader," *Financial Times*, 31 October 2016, accessed 28 October 2019, https://www.ft.com/content/39da343a-9f4b-11e6-891e-abe238dee8e2.

99. Rajendra Jadhav and Aftab Ahmed, "Shun Malaysia, India's palm oil buyers told amid Kashmir standoff," *Reuters*, 21 October 2019, accessed 22 October 2019, https://www.reuters.com/article/india-malaysia-trade/shun-malaysia-indias-palm-oil-buyers-told-amid-kashmir-standoff-idINKBN1X01J1.

100. "Q. *339 Trans-Karakoram Pass," Ministry of External Affairs, Government of India, 14 December 2006, accessed 28 October 2019,

https://www.mea.gov.in/rajya-sabha.htm?dtl/8120/q+339+transkarakoram+pass.

101. W.M. Dobell, "Ramifications of the China-Pakistan Border Treaty," *Pacific Affairs*, 37, no. 3 (Autumn, 1964): 283-295, Pacific Affairs, University of British Columbia Stable, accessed 28 October 2019, https://www.jstor.org/stable/2754976.

102. "Annual Report 2018-19," Ministry of Home Affairs, Government of India, accessed 30 October 2019, https://mha.gov.in/sites/default/files/AnnualReport_English_01102019.pdf.

103. Commodore Katherine Richards, "China-India: An analysis of the Himalayan territorial dispute," *Indo-Pacific Strategic Papers*, The Centre for Defence and Strategic Studies, February 2015, accessed 30 October 2019, https://www.defence.gov.au/ADC/Publications/IndoPac/Richards%20final%20IPSD%20paper.pdf.

104. Manoj Joshi, "The Wuhan summit and the India–China border dispute," Observer Research Foundation, 26 June 2018, accessed 21 October 2019, https://www.orfonline.org/research/41880-the-wuhan-summit-and-the-india-china-border-dispute/.

105. Harsh Pant, "The limits of informality," Observer Research Foundation, 14 October 2019, accessed 21 October 2019, https://www.orfonline.org/research/the-limits-of-informality-56585/.

106. ANI, "Modi accepts Xi's invitation for third informal summit in China," *India Today*, 12 October 2019, accessed 21 October 2019, https://www.indiatoday.in/india/story/modi-accepts-xi-jinping-invitation-third-informal-summit-china-1608717-2019-10-12.

107. Sanjeev Miglani, Neha Dasgupta, "Exclusive: China warns India of 'reverse sanctions' if Huawei is blocked – sources," *Reuters*, 6 August

2019, accessed 26 September 2019, https://in.reuters.com/article/huawei-india/exclusive-china-warns-india-of-reverse-sanctions-if-huawei-is-blocked-sources-idINKCN1UW1EY.

108. IANS, "Only 100% indigenisation can make India secure in 5G era: IIT Professor," *The Economic Times*, 11 July 2019, accessed 26 September 2019, https://telecom.economictimes.indiatimes.com/ news/only-100-indigenisation-can-make-india-secure-in-5g-era-iit-professor/70167675.

109. "Focus Areas," Centre of Excellence in Wireless Technology, accessed 1 October 2019, https://cewit.org.in/focus-areas/.

110. "Indigenous 5G TestBed: Building an end to end 5G Test Bed in India," Department of Computer Science & Engineering, Indian Institute of Technology Madras, accessed 1 October 2019, https://www.cse.iitm.ac.in/project_details.php?arg=MTcz.

111. Paul Triolo and Kevin Allison, "Eurasia Group White Paper: The Geopolitics of 5G, Eurasia Group," 15 November 2018, accessed 25 October 2019, https://www.eurasiagroup.net/siteFiles/Media/files/1811-14%205G%20special%20report%20public(1).pdf.

112. "Union Cabinet approves revival plan of BSNL and MTNL and in-principle merger of the two," Press Information Bureau, Government of India, 23 October 2019, accessed 25 October 2019, https://pib.gov.in/PressReleseDetail.aspx?PRID=1588848.

113. "Improving Quality Education," Press Information Bureau, Ministry of Human Resource Development, Government of India, 5 February 2018, accessed 1 October 2019, https://pib.gov.in/newsite/PrintRelease.aspx?relid=176204.

114. Katherine Koleski and Nargiza Salidjanova, "China's Technonationalism Toolbox: A Primer," U.S.-China Economic and

Security Review Commission, 28 March 2018, accessed 1 October 2019, https://www.uscc.gov/sites/default/files/Research/China%27s%20Technonationalism.pdf.

115. Richard J. Samuels, "Reinventing Security: Japan since Meiji," *Daedalus*, 120, no. 4, Searching for Security in a Global Economy (Fall 1991): 47-68, The MIT Press on behalf of American Academy of Arts & Sciences, accessed 1 October 2019, https://www.jstor.org/stable/20025403.

116. Evan A. Feigenbaum, "Soldiers, Weapons and Chinese Development Strategy: The Mao Era Military in China's Economic and Institutional Debate," *The China Quarterly*, no. 158 (June 1999): 285-313, Cambridge University Press on behalf of the School of Oriental and African Studies, accessed 1 October 2019, https://www.jstor.org/stable/656082.

117. Dieter Ernst, "Europe's Innovation Union— Beyond Techno–Nationalism?," *East-West Center Working Papers*, no. 132, August 2012, accessed 1 October 2019, https://www.eastwestcenter.org/system/tdf/private/econwp132.pdf?file=1&type=node&id=33627.

118. Nathan Gardels, "How tech may trip the Thucydides Trap," *The Washington Post*, 18 May 2018, accessed 29 November 2019, https://www.washingtonpost.com/news/theworldpost/wp/2018/05/18/china-technology-2/.

119. Nils Gilman, "China, Capitalism, and the New Cold War," *The American Interest*, 18 November 2019, accessed 29 November 2019, https://www.the-american-interest.com/2019/11/18/china-capitalism-and-the-new-cold-war/.

120. Nishant Ketu, "Data protection bill to come to parliament very soon: Prasad," *ANI*, 14 October 2019, accessed 2 November 2019, https://www.aninews.in/news/national/general-news/data-

protection-bill-to-come-to-parliament-very-soon-prasad20191014235707/.

121. Japnam K. Bindra, "SC backs DoT's revenue call in ₹ 92,000 cr blow to telcos," *Livemint*, 24 October 2019, accessed 2 November 2019, https://www.livemint.com/industry/telecom/sc-backs-dot-s-revenue-call-in-92-000-cr-blow-to-telcos-11571940733908.html.

122. Harsh Pant, "India is right to engage with China. But it has sent out signals of displeasure," Observer Research Foundation, 11 October 2019, accessed 22 October 2019, https://www.orfonline.org/research/india-is-right-to-engage-with-china-but-it-has-sent-out-signals-of-displeasure-56485/.

**Observer Research Foundation (ORF)** is a public policy think tank that aims to influence the formulation of policies for building a strong and prosperous India. ORF pursues these goals by providing informed and productive inputs, in-depth research, and stimulating discussions. The Foundation is supported in its mission by a cross-section of India's leading public figures, including academic and business leaders.


**Ideas • Forums • Leadership • Impact**

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-35332000 Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org