43

ORF SPECIAL REPORT

SEPTEMBER 2017

Breaking Free of the Digital Dragon: Responding to China's Growing Control Over India's ICT

Ojasvi Goel and Yash Bajaj

Source: quora.com

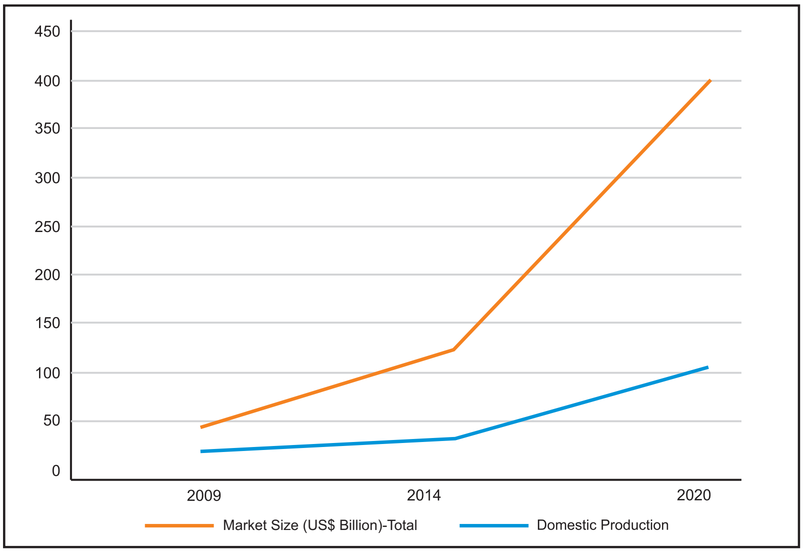
INTRODUCTION

India is poised to become one of the world's fastest growing consumers of electronics over the next five years, with domestic imports expected to reach over US$400 bn by 2020.[1] At the same time, the country is becoming increasingly dependent on information and communication technologies, and

ISBN 978-81-935589-1-1

the government has launched several initiatives for rapid digitisation. India, however, lags behind global competitors in its production capabilities, and 75 percent of that demand is projected to be fulfilled by imports – almost certainly dominated by China, which already supplies half of India's electronics imports.[2] This dependence has the potential to create economic and security-related vulnerabilities for India, and is made complicated by its geopolitical contestations with China. This report explores the extent of India's dependence on Chinese technology products and analyses the vulnerabilities created by them. It suggests several linked responses to the threat, core among them being a unified, strategic mindset.

Fig. 1: Projected demand-supply gap of electronic goods (US$ bn)



Source: ICICI Securities

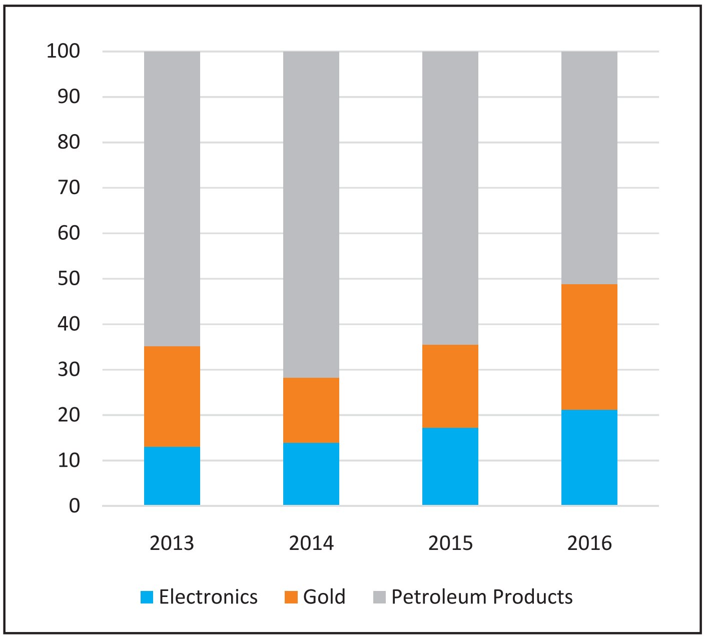
This report builds on some of the key themes discussed during a roundtable on India's insecurities in the electronics industry, organised by the Observer Research Foundation on 20 July 2017. The ideas shared by the participants form a key part of the report's recommendations.

DEPENDENCIES

India is becoming exponentially more connected through technology over the years, and by 2021, 59 percent of Indians will be internet users, up from only 28 percent in 2016. Already, India is the second largest mobile handset market in the world, and estimates suggest that a billion further smartphones will be sold by 2021.[3] This means that India requires commensurate growth in the production of telecommunications and wireless infrastructure, as well as in personal electronics, like smartphones. In addition, the government is investing heavily into its 'Smart Cities' initiative, which includes "robust IT connectivity and digitization" in its remit.[4] These too will require a significant supply of electronics – most of which India currently lacks the indigenous capability to meet.

The shortfall is evidently growing: electronics imports are already the third most valued category of imports for India, and the country's import bill of electronics goods (US$37bn in 2016[5]) has recorded a compound annual growth rate (CAGR) of 18.3 percent over the past 15 years, higher than the import bill of petroleum products and gold, which grew at a CAGR of 16.8 percent and 16.4 percent, respectively.[6] Taxation policy has been blamed for poor economic incentives to produce domestically, and despite the feted 'Make in India' scheme, India lacks a robust manufacturing ecosystem to serve its burgeoning demand. Its neighbour, China, on the other hand, boasts perhaps the strongest such ecosystem globally, and Chinese firms have already made significant inroads into supplying the Indian electronics market. Notably, in 2016, electronics imports from China alone contributed US$20bn to India's trade deficit of US$96bn.[7] The extent of this dependence, and China's steps towards increasing their share in India and abroad are detailed in the subsections, divided by broad sectors.

Fig. 2: Import composition of three major commodities (in %)



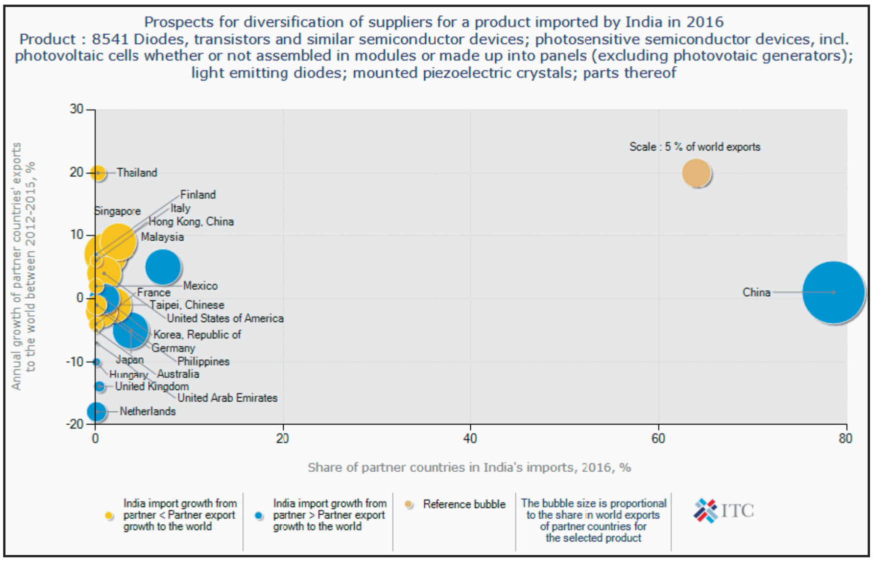
Source: ITC Trade Map

Across all sectors, outbound mergers and acquisitions deal flow from China have risen consistently, with technology driving this increase substantially. In 2016, Chinese firms spent almost US$40bn on investments in foreign technology companies.[8] While the Chinese government has cooled overall outbound M&A projections by implementing new regulations to prevent capital flight, it is unlikely that this will significantly affect strategic investments, under which most technology deals fall.[9] The consensus is that these purchases are to acquire foreign technology and intellectual property, for Chinese firms to effectively compete on the global stage.[10]

SEMICONDUCTORS

Semiconductor devices, including integrated circuits, form the backbone of all electronic devices, serving as connectors for various components. India's Ministry of Electronics & Information Technology acknowledges that there is currently no production of these components in India.[11] Two fabrication units planned in 2014 are stalled due to difficulties securing investors, but the government remains committed to eventually manufacturing semiconductors domestically, since demand is set to rise to US$55bn by 2020.[12] As it stands, China makes 78 percent of the semiconductors used in India, in addition to making 30 percent of its electronic circuitry imports.[13]

Fig. 3



This is in stark contrast to the rest of the world. For instance, China has only a 16.2 percent share in the worldwide semiconductor market.[14] It is, however, investing in growing their capabilities both in capacity and in quality. In 2014, China launched a set of national guidelines for the development and promotion of their indigenous semiconductor manufacturing capabilities. Overall, an investment of around US$150 bn is projected until 2030, and with the stated goal of high self-sufficiency in the sector, a perceived necessity due to China's surging demand for semiconductors.[15] In comparison, India has only earmarked a US$10-bn investment to create two semiconductor plants.[16] To compete in terms of quality, Chinese firms have looked abroad, both acquiring and partnering with foreign firms to boost indigenous intellectual property.

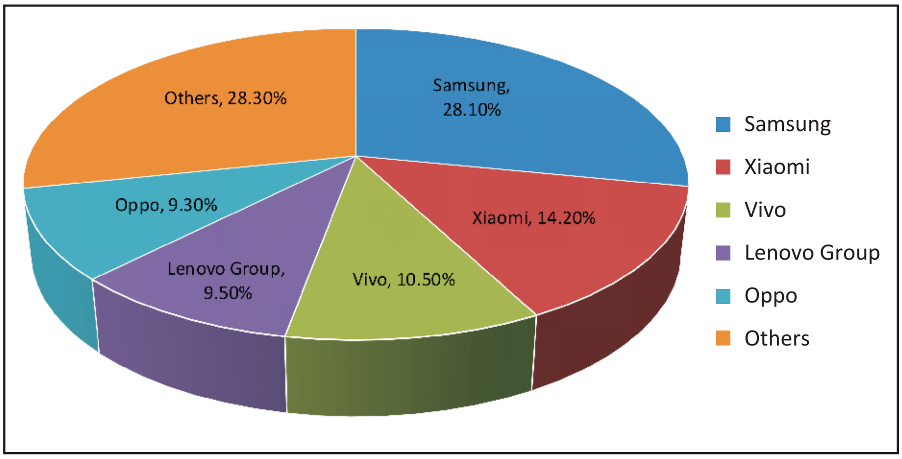
Tsinghua Unigroup, which has begun building a US$30-bn memory-chip production complex in China, recently teamed up with Britain's Dialog Semiconductor to jointly design communications components.[17]

Some of China's forays abroad have been met with opposition from foreign governments, with reservations raised over security concerns, and protests against purported anticompetitive behaviour. In December 2016, then US President Barack Obama blocked the sale of the American divisions of Aixtron, a German semiconductor manufacturer, on security grounds. The stated justification for the block was that Aixtron produced technology that had military applications, and so any acquisition would threaten national security.[18] Just a month after that decision, the US President's Council of Advisors on Science and Technology (PCAST) released a report on semiconductor manufacturing worldwide.[19] It highlighted China's 'concerted push' into the industry via government backing and industrial policy, and urged the US government to act against China's market-distorting behaviour, which includes heavy subsidies to domestic producers and stealing intellectual property. India has reacted to China's anticompetitive behaviour in the past, most recently imposing an anti-dumping duty on tempered glass, one of the key components in smartphones.[20] One of the recommendations of the PCAST is that the US begin to use national security protocols as a mechanism of action against these.

Consumer electronics and software

Semiconductors and integrated circuits form around a quarter of the material cost of smartphones,[21] another industry in which Chinese firms have taken the ascendancy in India. Three of the top five handset brands are Chinese (Xiaomi, Oppo, and Vivo), and the other two are foreign as well – the fourth quarter of 2016 was the first in which no Indian manufacturer was represented in the top five. Indeed, Chinese firms had a market share of over 50 percent, and were by far the fastest growing firms as well.[22] Oppo and Vivo are both marque products of Guangdong-based BBK Electronics, which became the second largest smartphone manufacturer in the world in the first quarter of 2017.[23] BBK also manufactures the well-known OnePlus brand. They have committed to spending around US$250m on marketing in India in 2017, launching an advertising blitz that includes billboards, sponsorships, and incentives to retail outlets.[24] They have also spent large sums on establishing their own retail presence in markets across India. The market perception is that Chinese firms are better equipped to respond to the demands of Indian consumers, and have adapted more quickly to 4G technology than their Indian counterparts.[25]

Fig. 4: Top Five Smartphone Companies in India



Source: IDC Quarterly Mobile Phone Tracker, May 16, 2017

Notes:

- *The 'Company' represents the current parent company (or holding company) for all brands owned and operated as subsidiary.*
- *Lenovo Group includes all three brands (Lenovo, Motorola, ZUK)*

While India is beginning to host some assembly units for these Chinese firms, the value added is very low, at around two to three percent. This is since almost all of India's assembly hubs are engaged in Semi Knocked Down (SKD) assembly – where only basic last-mile assembly and packaging is done in the country while populated and mounted Printed Circuit Boards (PCBs) and other sub-assemblies are imported.[26] Indian phonemakers are deeply worried about China's growing ascendancy in this sector, and have called for the government to take strong actions against Chinese firms.[27]

Further, Chinese smartphones tend to run Chinese browsers – in particular, Alibaba's UCBrowser, which now holds over 50 percent of the browser market share in India.[28] Alibaba also runs UCNews, a curated news platform, which crossed 100 million users in India and Indonesia in 2017. Indian smartphone users on average spend around 160 minutes a day using different apps,[29] and Alibaba says that an average user of UC News spends around 25 minutes a day on the app.[30] This opens the possibility that UCNews has captured a large portion of the overall time spent by Indians on the internet, which is only likely to rise further in the future.[31]

Alibaba has also taken a large stake in Paytm, India's leading e-payments app. Paytm has launched a payments bank, and the firm may soon be majority-controlled by Chinese investors, with reports that they are looking to raise their stake to 70 percent.[32] India's demonetisation drive in late 2016 drove traffic to the app, and as of February 2017, 200 million people hold wallets with the service.[33]

Wireless and core infrastructure

A significant portion of India's wireless and telecommunications infrastructure is procured from the Chinese companies ZTE and Huawei.[34] They are also beginning to take more active roles in network management and operations. In October 2016, Huawei secured a managed services contract from Vodafone, India's second largest telecom operator. This includes network operations across much of the south of India and in India's capital, New Delhi. This would give Huawei access and potential control over sensitive and critical communications.[35] That deal succeeded another one with market leader Airtel, where Huawei provided expertise in broadband network upgrades.[36] These managed services operations were dominated by Ericsson and Nokia, but Huawei has made significant inroads into the market in India. Indian firms lack the technological capacity to serve these networks by themselves, and therefore some foreign reliance is necessary.

The Indian government has, in the past, acknowledged that such telecommunications infrastructure can be used improperly, and in April 2010 blocked mobile operators from importing any further equipment from Chinese vendors. This ban followed concerns raised by the Home Ministry that such equipment could contain spyware that may be abused by China.[37] The ban was overturned in June 2010, however, after concerns that the freeze would negatively impact India's 3G adoption.[38]

While not necessarily dominant, Huawei is also bidding for several Smart City projects in India – the company has bid for or already advised around a hundred cities in over 40 countries.[39] In its other Smart City projects, Huawei has placed a heavy focus on public safety via video-analysis, monitoring, and wireless networks for police services.[40,41] Some of its systems include 'rapid deployment of video surveillance networks', as in the French city of Valenciennes. There, Huawei deployed 217 cameras and upgraded their monitoring system. It remains to be seen whether such functions will be a part of their ambit should they secure projects in India, but it is worth noting that Smart Cities Council India describes video surveillance as "vital" for smart cities.[42]

Chinese firms are also interested in power and military-related infrastructure. A panellist at the ORF roundtable brought attention to a recent tender by Bharat Sanchar Nigam Ltd, India's state-owned communications company, for submarine communication cables. The tender was open to firms worldwide, and included contracts for cables that would be used for confidential military communications.[43] Chinese firms including Huawei are likely to bid, and it remains to be seen who will win the contract.

VULNERABILITIES

The cross-sectoral dependence on and influence of China should be worrying for India. It can be argued that excessive dependence on a single economy is in itself undesirable – but given India and China's ongoing geopolitical contests over connectivity projects as well as their boundary disputes, this dependence could well translate into potential vulnerabilities. The reach of Chinese technology into the Indian market creates multiple pressure points through which they can block and mediate the use of technology-driven services and information across public channels. Some of these pressure points and vulnerabilities are economic, but others are security-related, and require urgent attention from policymakers.

Economic issues

On the economic front, the rising spiral of high electronics imports continues to negatively skew India's precarious balance of trade, despite the persistence of low crude oil prices. Illustratively, from 2014 to 2015, although the crude oil import bill for India came down by about US$40bn, India's trade deficit improved by only US$15bn.[44] The consistently higher growth rate for electronics imports has created short intervals in which the import bill of electronics has surpassed the import bill of gold. In April 2017, for instance, electronic imports outstripped gold imports by about US$600m.[45] Failure to take corrective action to contain the dependency on imports to satiate India's demand for electronics might inflate its electronics import bill such that it surpasses its oil bill by 2020, as is being increasingly reported.[46] If India's import bill continues to rise, it would require much larger purchases of foreign exchange reserves in order to maintain a healthy import cover – which could squeeze currency prices and potentially trigger a balance-of-payments crisis. While this remains a distant threat, it is something that bears consideration if electronics demand continues to grow and is supplied from abroad.[47]

Embargo is another risk from import dependence – since India imports the lion's share of its semiconductors and other electronic raw materials from China, it is possible for them to suddenly halt Indian industries that use them. It has done so with strategically important export goods in the past, such as rare earth metals, which it restricted Japanese imports of in response to political disagreements in the South China Sea.[48] While an international effort forced China to drop its export quotas on the metals after three years, this situation indicates that China considers, and has used, embargos as a political tool, something that could seriously harm India's industrial aspirations.[49]

Critical infrastructure attacks

The Chinese People's Liberation Army (PLA) has been accused repeatedly of targeting foreign countries with cyber-attacks.[50] While the focus of Chinese cyber-attacks was on industrial espionage in the past, the Director of the United States' National Security Agency said in 2014 that China had the capability to shut down power utilities and financial companies there.[51] India too is vulnerable to such attacks, and its vulnerabilities are amplified by the dependence on Chinese technology.[52] As mentioned earlier, most of India's wireless infrastructure is already provided by Chinese firms, which lays open the possibility of possible backdoors to manipulate them from abroad. Huawei's managed services contracts, for example, allow the company direct control over telecommunications networks.[53]

The problems are exacerbated by the close links between the Chinese state and technology companies – the founder of Huawei was himself in the PLA. A 2012 report by the US Permanent Select Committee on Intelligence discussed in detail the links between Huawei, ZTE, and the PLA. One of its key findings was that Huawei likely engaged in R&D on behalf of the PLA, and provided its services to a cyber-warfare unit.[54] Indeed, India's own National Security Council Secretariat warned in 2013 that Huawei and ZTE were part of a PLA project, and highlighted ZTEs contract for the Power Grid Corporation of India as problematic. They raised concerns that Chinese firms could deny timely service in the event of breakdowns, and that malicious hardware could be exploited in any future conflict with India.[55]

If Chinese companies are granted smart cities contracts and allowed to manage other core infrastructure, the Chinese state could have a facile way of controlling and compromising that infrastructure. This is unacceptable, and a severe threat to Indian security.

Surveillance

Article 11 of the Chinese State Security Law reads: "a State security organ may inspect the electronic communication instruments and appliances and other similar equipment and installations belonging to any organization or individual."[56] This permits the Chinese government to access all the data of firms headquartered in China, which means that all data collected by Chinese phones in India is readily available as well. In addition, the Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE (2012) mentions that there is a grave threat of surveillance backdoors built into telecommunications infrastructure. If

Chinese firms are engaged in providing video surveillance capabilities in smart cities, as they have done elsewhere, this creates even more avenues for the Chinese intelligence establishment to monitor the activity of Indians. Other American technology analysts have echoed these sentiments, with Michael Maloof, a former analyst in the Office of the Secretary of Defense, saying that both Huawei and ZTE create backdoors in their technology to facilitate Chinese espionage.[57]

In November 2016, Kryptowire discovered backdoors in firmware developed by China-based Shanghai Ad Ups Technology pre-installed on over 700 million phones.[58] In 2015, German cyber-security companies found pre-installed malware that could listen to calls, track users, and make online purchases on smartphones from Chinese companies including Huawei and Xiaomi.[59] In 2013, the former chief of the US Central Intelligence Agency (CIA) Michael Hayden, remarked that China's telecom giant Huawei "is a significant security threat" and has spied for the Chinese government.[60] Also in that year, Huawei phones were banned from use in Australia's National Broadcasting Network, due to advice from Australian intelligence agencies.[61] It is entirely possible, if not altogether likely, that new Chinese smartphones exported to India serve as a method for the Chinese military and intelligence apparatus to gain crucial information on India.[62] Both the law, and the Chinese practice of 'picking winners' from within its domestic private industry means that Chinese firms will likely feel pressured to obey government requests, including for installing backdoors and more. China already engages in mass surveillance of its own population – indeed, when AdUps was reached for comment about the backdoors, they said that "it was not intended for American phones", but was an intentional piece of software designed for a Chinese phone manufacturer.[63] As previously mentioned, India's home ministry has raised concerns about Chinese spyware being present in telecommunications technology, but economic concerns overrode a ban on the technology in 2010.

With this extent of control, malware and security bugs in Chinese software are not even necessary for the Chinese state to obtain important Indian data. However, some dependencies on Chinese technology make India especially vulnerable. Security liabilities have been found in UCBrowser – Canada's CitizenLab found serious data and privacy issues with the browser in 2015. This included unencrypted search queries, location data and device identifiers.[64]

In sum, if China does not already engage in surveillance of targets within India, it has the capability to do so. Its capabilities are bolstered every time an Indian purchases a Chinese smartphone, or another component of telecommunications infrastructure is imported from China. This puts India at a distinct informational disadvantage, and it means that Chinese intelligence is likely extremely well informed about strategic trends in the market and among the population – perhaps more so than India itself.

Propaganda and cultural influence

China's control over India's information and communication technologies allows it to surveil India's population and also gives it the potential capacity to disrupt infrastructure. Further, however, it opens up the possibility for the Chinese state to use their now well-established Indian platforms to spread propaganda and misinformation, which is a risk previously overlooked in the literature.

China operates a formidable propaganda machine, blending traditional media with diplomacy, games, and social media. Its goals include telling a "good Chinese story" and emphasising what it claims is China's desire for peaceful ascendancy in the world order.[65]Online, it has an army of youths who trawl the internet, refuting criticism of the Chinese Communist Party – the 50 Cent Party, named for the amount of Chinese cents they receive per post.[66] This group is estimated to comprise over two million people, and studies estimate that one in every 178 posts on the Chinese internet are created by government employees.[67]

While propaganda inside China is stronger than it is outside, the increasing use of UCNews and UCWeb inside India could provide a route for Chinese propaganda officials to influence Indians. In April 2017, Indian MP Prahlad Patel raised UCBrowser in Parliament, describing pervasive censorship by the browser on issues deemed sensitive to the Chinese government, including that of Tibet. He also highlighted UCNews as a platform for Chinese propaganda.[68] Searches on the curation service indicated no coverage of the Dalai Lama and unsympathetic coverage of Taiwan. If, as mentioned above, the average UCNews user spends 25 minutes a day on the app, China can command the interest of, and inject news stories directly to tens of millions of Indians.

Alibaba, the owner of these firms, is no less connected to the Chinese military establishment than Huawei or ZTE – they entered a joint venture with Norinco, a state-owned arms producer, in 2015 to develop satellite navigation capabilities.[69] Worryingly, its owner, Jack Ma, recently purchased the *South China Morning Post*, a prestigious Hong Kong newspaper. Analysts suggest that his intention is to "tell China's story more positively", suppressing critical news.[70] If Mr. Ma is truly committed to this ideal, as his large bonuses to retain SCMP staff indicate,[71] there is nothing stopping him from cultivating UCNews into an even more effective tool for projecting Chinese influence. This, of course, would provide control over geopolitical narratives to the Chinese state as well, which is again a significant vulnerability for the Indian state.

RESPONSES

The discussants at ORF's roundtable agreed that the problems posed by these vulnerabilities were severe and demanded active responses by Indian policymakers. They stressed the necessity of reducing India's dependence on Chinese electronics to bring down the magnitude of these vulnerabilities. Doing so requires the demand gap to be met somehow else, and so India's responses must both work to curtail Chinese influence and increase domestic production. Attempts have been made by the government to slowly limit the ambit and extent of Chinese influence, atleast in the smartphones ecosystem. The Ministry of Electronics and Information Technology (MeitY) has asked 21 smartphone makers, most of them Chinese, to provide details about the safety and security practices, architecture frameworks, guidelines, standards, among others, followed in their product/services in the country.[72] Media reportage also indicates that the government is contemplating asking these Chinese handset makers to set up servers in India as the next step in ensuring the protection of user data, following concerns about security breaches, given that most Chinese smartphone vendors presently have servers in their home country.[73]

The key step is for India to deal with this issue with a strategic mindset, like how it approached building its nuclear capabilities. A unified front must be developed across ministries, since the responses require the input of financial, trade, technological and security experts. In fact the National Policy on Electronics (NPE), launched in 2012, was an attempt to steer towards multistakeholderism, with its focus on working in conjunction with Central ministries like Telecom, MSME and IT, and State governments like Andhra Pradesh and Karnataka.[74] Recently, the Electronics and IT Minister announced plans to unveil a new policy for electronics and software production, as well as for data protection and setting up startup clusters.[75] This will broaden the mandate of the NPE-12, and open up avenues to engage with a larger number of stakeholders. A free flow of information between these stakeholders will allow, for example, harmonisation between trade and security policy, so that security concerns around imports are adequately addressed in international trade agreements.

Trade Policy

Smart trade policy steps will ensure that fledgling Indian manufacturers can compete in their own market. To this extent, suggestions included the introduction of strong non-tariff barriers on electronic goods. This is not dissimilar to the proposal presented to former US President Obama, where national security grounds were discussed as market protection measures. This will largely be reciprocal – China imposes several such barriers on India exports at present.[76] In addition, product-specific safeguards on imports and exports should be negotiated in free trade agreements, like the Regional Comprehensive Economic Partnership (RCEP), to stem imports beyond a certain limit from certain countries and protect domestic production. Frequent RCEP negotiation rounds, including the one that happened in July this year, are opportune platforms to raise such demands. Even industry associations like CII and FICCI need to flag the issue of product-specific safeguards at appropriate fora like Empowered Committee meetings, when such inputs are solicited.

Trade diplomacy can also have more overt security benefits – negotiations around the now-failed Trans-Pacific Partnership discussed data localisation requirements, which would allow countries to protect their data. The mainstreaming of the discourse on data protection and privacy in the country, through the landmark Supreme Court judgment on Right to Privacy and also through Telecom Regulatory Authority of India's (TRAI) consultations on data protection, is emblematic of the government's increasing focus on data protection. Source code disclosure was also mooted as a prerequisite for import permission, which would presumably secure software given adequate testing facilities.

Taxation Policy

India must also create a taxation environment conducive to manufacturing, both for semiconductors and consumer goods, like smartphones. The focus must be on establishing higher value Completely-Knocked-Down (CKD) assembly with testing facilities, and moving away from SKD facilities. Currently, there exist perverse incentives that push manufacturers towards opting to import finished products into the country. Under the present GST regime, mobile phones manufactured in India will be taxed at 12 percent, while those imported as Completely Build Units (CBUs) will be taxed at 12 percent plus 10 percent of Basic Custom Duty (BCD). However, GST on import of populated, loaded or stuffed PCB is 18 percent while import of other components is taxed at 18 percent plus 10 per cent of BCD. Clearly, the taxation regime incentivises manufacturers to import CBUs over SKDs and CKDs thereby inhibiting the capture of a larger value for local manufacturing. Concerted efforts are required to make importing CBUs least profitable for the manufacturers. Parallels can be drawn with the country's luxury car market where through the imposition of higher taxes on imported luxury cars, the government forced most major automobile manufacturers to set up CKD assembly units within the country.

Norm Building and Diplomacy

The strategic mindset must extend to the international arena, and India must form a coherent narrative on cybersecurity that it wishes to advance internationally. Chinese firms are already moving forward in trying to set the global paradigms on this – Huawei, for one, has released several white papers on the subject. If India wants to protect its interests, which in many cases are diametrically opposed to those of China in this realm, it must take an active role in promoting global norms that work in its favour. To this end, discussions about policy priorities must take place and be lobbied for with global technology leaders as well. Already, several prominent countries are frustrated with and wary of Chinese manoeuvres in the high-tech space. India should capitalise on this sentiment and seek to offer itself as an alternate destination for partnerships, as well as discuss global economic and political responses to China's dominant position.

CONCLUSION

India requires increasing amounts of technology to succeed as a nation with its economic, social and political objectives. It must ensure that this dependence and growth does not leave it vulnerable to capricious foreign powers and should view the electronics and telecommunications sectors with a strategic mindset.

India must advance on several fronts: first, this report recommends that the government set up a high-level, multi-stakeholder group tasked with solving issues around India's dependence on Chinese electronic goods. That group must then create change both at home and abroad. Domestically, taxation policy must be adequately rationalised to incentivise Indian manufacturing over imports. Resources must be dedicated towards creating a strong supply chain for electronics goods, most efficiently done by collaborating with friendly and more technologically advanced countries. Abroad, India must work to ensure its security concerns are adequately addressed in multilateral trade agreements, by enforcing heavier non-tariff barriers on foreign goods, or allowing for exceptions based on national security grounds. India must also work towards setting global norms on cybersecurity for its interests to be met – capitalising on the global discontent with Chinese actions in the space.

Only a strong, concerted effort by India to harmonise its own policies and mobilise the global community will the country be able to withstand China's efforts to control the Indian market. It is of utmost importance that India make that effort.

ABOUT THE AUTHORS

Ojasvi Goel is a student of economics at the London School of Economics and Political Science. He worked on this report while interning at ORF.

Yash Bajaj is a Programme Associate at Koan Advisory Group, New Delhi. Prior to this, he assisted a Member of Parliament from Telangana as part of the LAMP Fellowship programme run by PRS Legislative Research.

ENDNOTES

1. "Electrical and Electronics Manufacturing in India Report,"ASSOCHAM-NEC Technologies, last modified May, 2017, http://www.nectechnologies.in/ en_TI/pdf/-AssochamReport-NTIasKnowledgePartner.pdf.
2. Press Trust of India,"Over half of electronic imports from China,". Business Standard, last modified April 27, 2016, http://www.business-standard.com/article/pti-stories/over-half-of-electronic-imports-from-china-116042700819_1.html.
3. "VNI Forecast Highlights 2016-2021," Cisco, last modified June, 2017, https://www.cisco.com/assets/sol/sp/vni/forecast_highlights_mobile/#~Country.
4. Ministry of Housing and Urban Affairs,"Smart Cities,"Government of India, August 13, 2017, http://moud.gov.in/cms/smart-cities.php.
5. Mundy, Simon,"India faces tough calls on local phone manufacturing," Financial Times, July 4, 2017, https://www.ft.com/content/5d3f24da-5693-11e7-9fed-c19e2700005f.
6. "Electronic goods: Demand set to surpass oil bill by 2020", ICICI Securities, December 18, 2015, http://content.icicidirect.com/mailimages/ElectronicsGoods.htm.
7. "Trade Map,"International Trade Centre, 2016, http://www.trademap.org/ Index.aspx.
8. "M&A 2016 review and 2017 outlook," PricewaterhouseCoopers China, 2016, https://www.pwccn.com/en/services/deals-m-and-a/publications/ma-2016-review-and-2017-outlook.html.
9. Mitchell, Tom,& Wildau, Gabriel, "China's State Council puts seal on capital controls," Financial Times, August 18, 2017, https://www.ft.com/content/ 3a638d1c-8405-11e7-a4ce-15b2513cb3ff.
10. Xinhua, "China TMT overseas M&A market to grow steadily in 2017: Deloitte,", China Daily, March 7, 2017, http://www.chinadaily.com.cn/business/2017-03/07/ content_28457128.htm.
11. "Semiconductor", Ministry of Electronics & Information Technology, Government of India, http://meity.gov.in/esdm/semiconductor.

12. Bhargava, Yuthika, "Revised semiconductor policy on anvil,"The Hindu, August 02, 2017, http://www.thehindu.com/business/Economy/revised-semiconductor-policy-on-anvil/article19409941.ece.

13. "M&A 2016 review and 2017 outlook," PricewaterhouseCoopers China, 2016, https://www.pwccn.com/en/services/deals-m-and-a/publications/ma-2016-review-and-2017-outlook.html

14. "M&A 2016 review and 2017 outlook," PricewaterHouseCoopers China, 2016, https://www.pwccn.com/en/services/deals-m-and-a/publications/ma-2016-review-and-2017-outlook.html.

15. Thomas, Christopher, "A new world under construction: China and semiconductors," McKinsey & Company, November,2015, http://www.mckinsey.com/global-themes/asia-pacific/a-new-world-under-construction-china-and-semiconductors.

16. Srivastava, Moulishree, "Govt plans $10 billion investment in two semiconductor plants," liveMint, March 26, 2015, http://www.livemint.com/Industry/ZRBFOTaucH1NO9el7JLZXJ/Govt-to-invest-10-billion-in-two-computer-chip-manufacturin.html.

17. "Apple-Supplier Dialog Will Develop Chips With China's Tsinghua," Bloomberg News, March 9, 2017, https://www.bloomberg.com/news/articles/2017-03-09/apple-supplier-dialog-will-develop-chips-with-china-s-tsinghua.

18. McLaughlin, David,"Obama Blocks Chinese Takeover of Aixtron as U.S. Security Risk," Bloomberg Markets, December 3, 2016, https://www.bloomberg.com/news/articles/2016-12-02/obama-blocks-chinese-takeover-of-aixtron-as-u-s-security-risk.

19. The President's Council of Advisors on Science and Technology, "Report to the President: Ensuring Long-Term U.S. Leadership in Semiconductors,"Washington D.C.: Executive Office of the President of the United States, 2017.

20. Press Trust of India,"India imposes anti-dumping duty on tempered glass from China," Times of India, August 21, 2017, http://timesofindia.indiatimes.com/business/india-business/india-imposes-anti-dumping-duty-on-tempered-glass-from-china/articleshow/60159189.cms.

21. "iPhone 7 Materials Costs Higher than Previous Versions, IHS Markit Teardown Reveals," HIS Markit, September 20, 2016, http://news.ihsmarkit.com/press-release/technology/iphone-7-materials-costs-higher-previous-versions-ihs-markit-teardown-revea.

22. Dhapola, Shruti, "In a first, no Indian smartphone manufacturer in IDC's top five list for Q4," The Indian Express, February 13, 2017, http://indianexpress.com/article/technology/tech-news-technology/idc-q4-2016-xiaomi-lenovo-chinese-players-dominate-indian-players-out-4522342/.

23. Manners, David , "BBK is second largest smartphone manufacturer," Electronics Weekly, May 26, 2017, https://www.electronicsweekly.com/news/business/bbk-second-largest-smarphone-manufacturer-2017-05/.

24. Mukherjee, Writankar, & Anand, Shambhavi, "Revealed: Oppo, Vivo's Rs 2,200 crore marketing strategy to overtake Samsung in India,"Economic Times, May 3, 2017, http://telecom.economictimes.indiatimes.com/news/revealed-oppo-vivos-rs-2200-crore-marketing-strategy-to-overtake-samsung-in-india/58488396.

25. S, Vidya, "Chinese firms out to capture India's mobile phone market,"Mail Today, August

1, 2017, http://indiatoday.intoday.in/story/china-india-mobile-phone-market-smartphones-xiaomi-vivo-lenovo/1/1015722.html.

26. "Maximizing Local Value Addition in Indian Mobile Phone Manufacturing: A Practical Phased Approach," IIM Bangalore-Counterpoint, November, 2016, http://www.iimb.ac.in/sites/default/files/research/files/workingpaper/WP%20No.%20528.pdf.

27. Mundy, Simon, "India's phonemakers cry foul on Chinese rivals," Financial Times, April 17, 2017, https://www.ft.com/content/6cb6405c-2276-11e7-8691-d5f7e0cd0a16.

28. Meeker, Mary,"Internet Trends 2017 - Code Conference," Kleiner Perkins Caufield Byers, May 31, 2017, http://www.kpcb.com/internet-trends.

29. "160 mins: Time Indian smartphone users spend on average 11 apps a day,"Techseen,http://techseen.com/2017/05/04/app-annie-indians-spend-160mins-apps/

30. Abbas, Muntazir,"Alibaba's UC News gets 100 million active users in India & Indonesia,"Economic Times, April 11, 2017, http://telecom.economictimes.indiatimes.com/news/alibabas-uc-news-gets-100-million-active-users-in-india-indonesia/58124591

31. ibid

32. "We're as Indian as Maruti: Paytm founder Vijay Shekhar Sharma on Chinese ownership," Press Trust of India, November 26, 2017, http://economictimes.indiatimes.com/small-biz/startups/were-as-indian-as-maruti-paytm-founder-vijay-shekhar-sharma-on-chinese-ownership/articleshow/55647880.cms

33. "Paytm crosses 200 million wallet user base," Business Standard, February 28, 2017,

34. Gupta, Surajeet Das, "Over 90% of telecom gear in India's Rs 50,000-cr market is imported,"Business Standard, April 29, 2014, http://www.business-standard.com/article/companies/over-90-of-telecom-gear-in-india-s-rs-50-000-cr-market-is-imported-114042900254_1.html

35. Khan, Danish, "Huawei bags three-year managed services contract from Vodafone India," The Economic Times, October 17, 2016, http://economictimes.indiatimes.com/tech/hardware/huawei-bags-three-year-managed-services-contract-from-vodafone-india/articleshow/54887189.cms

36. Khan, Danish, "Huawei wins $120 million contracts to upgrade Airtel, Idea wireline networks," The Economic Times, January 21, 2015, http://telecom.economictimes.indiatimes.com/news/infrastructure/telecom-equipment/huawei-wins-120-m-contracts-to-upgrade-airtel-idea-wireline-networks/45948486

37. Thomas, K. "Govt bans import of Chinese telecom equipment,"The Hindu BusinessLine, April 28, 2010,http://www.thehindubusinessline.com/todays-paper/govt-bans-import-of-chinese-telecom-equipment/article990404.ece

38. Putcha, Shiv, & Grivolas, Julien,"India lifts ban on Chinese telecom vendors,"Telecom Asia:, June 7, 2010, https://www.telecomasia.net/content/india-lifts-ban-chinese-telecom-vendors

39. "Huawei keen on India's smart city project: official,"Deccan Chronicle, April 19, 2017, http://www.deccanchronicle.com/business/companies/190417/huawei-keen-on-indias-smart-city-project-official.html

40. "Huawei Releases eLTE SafeCity Solution for Public Safety," Huawei, May 18, 2017, http://www.huawei.com/en/news/2017/5/eLTE-SafeCity-Solution

41. "Public Safety", Huawei, 2017, http://e.huawei.com/in/solutions/industries/public-safety

42. "Here's Why Surveillance is Vital for Smart Cities,"Smart Cities Council India, January 27, 2017, http://india.smartcitiescouncil.com/article/here%E2%80%99s-why-surveillance-vital-smart-cities

43. Singh, S. R., & Nayanimabasu. "Red alert of Chinese firms eyeing BSNL cable project",The Hindu BusinessLine, July 12, 2017,http://www.thehindubusinessline.com/info-tech/red-alert-over-chinese-firms-eyeing-bsnl-cable-project/article9763354.ece

44. "Trade Map," International Trade Centre, 2016, http://www.trademap.org/Index.aspx.

45. Mishra, Asit Ranjan, "Are electronic imports the new gold for the Indian economy?,"LiveMint, May 18, 2017, http://www.livemint.com/Politics/LfLrcWeYj6UXN5leAYyEWI/Are-electronic-imports-the-new-gold-for-the-Indian-economy.html

46. "Electronic goods: Demand set to surpass oil bill by 2020," ICICI Securities Market Wrap, December 18, 2015, http://content.icicidirect.com/mailimages/ElectronicsGoods.htm

47. "Trade deficit with China an issue of concern: Govt.,"The Hindu Business Line,July 24, 2017,http://www.thehindubusinessline.com/economy/trade-deficit-with-china-an-issue-of-concern-govt/article9786089.ece

48. "China - Rare Earths," World Trade Organization, 2017, https://www.wto.org/english/tratop_e/dispu_e/cases_e/1pagesum_e/ds431sum_e.pdf

49. "Boycott of Chinese goods: China warns of impact on India-bound investments,"The Times of India, October 27, 2016, : http://timesofindia.indiatimes.com/world/china/Boycott-of-Chinese-goods-China-warns-of-impact-on-India-bound-investments/articleshow/55096140.cms

50. Gertz, Bill,"China Continuing Cyber Attacks on U.S. Networks,"The Washington Free Beacon,March 18, 2016,http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/

51. Zengerle, Patricia, "NSA chief warns Chinese cyber-attacks could shut U.S. infrastructure," Reuters, November 21, 2014,http://www.reuters.com/article/us-usa-security-nsa-idUSKCN0J420Q20141121

52. Timmons Heather,"India tells mobile firms to delay deals for Chinese Telecom Equipment,"The New York Times, April 30, 2010, http://www.nytimes.com/2010/05/01/business/global/01delhi.html?mcubz=0

53. "Huawei India – Services", http://www.huawei.com/in/services/hw-u_256734.htm

54. Rogers, M., & Ruppersberger, C. D., Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, October 8, 2012, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

55. Philip, Joji Thomas,"NSC points to Huawei, ZTE's links with Chinese military,"The Economic Times, May 15, 2013, http://economictimes.indiatimes.com/news/politics-and-nation/nsc-points-to-huawei-ztes-links-with-chinese-military-project-pla-863/articleshow/20056800.cms

56. "State Security Law of the People's Republic of China," People's Republic of China, 1993, http://www.china.org.cn/english/China/218754.htm

57. Protalinksi, Emil, "Former Pentagon analyst: China has backdoors to 80% of telecoms,", Zero Day, July 14, 2012, http://www.zdnet.com/article/former-pentagon-analyst-china-has-backdoors-to-80-of-telecoms/

58. "Indian Android smartphones are at data theft risk: Experts,"The Indian Express, November 23, 2016, http://indianexpress.com/article/technology/mobile-tabs/indian-android-smartphone-users-too-at-data-theft-risk-experts-4391569/

59. Philipp, J. "Spy Software Found Preinstalled on Lenovo, Huawei and Xiaomi Smartphones," The Epoch Times, September, 2015: http://www.theepochtimes.com/n3/1748900-spy-software-found-pre-installed-on-lenovo-huawei-and-xiaomi-smartphones/

60. Tiwary, Deeptiman, "Huawei a threat, it spies for China: Ex-CIA chief,"The Times of India,July, 2013, http://timesofindia.indiatimes.com/world/us/Huawei-a-threat-it-spies-for-China-Ex-CIA-chief/articleshow/21206193.cms

61. Remeikis, Amy, & Massola, James, "Chinese firm Huawei banned from NBN supplying phones to Australia Defence,"The Sydney Morning Herald,June 18, 2017, http://www.smh.com.au/federal-politics/political-news/chinese-firm-huawei-banned-from-nbn-supplying-phones-to-australia-defence-20170616-gwsne4.html

62. Rao, Rajiv, "India accuses Huawei of hacking into its telecom network,", Zero Day Net, February 7, 2014, http://www.zdnet.com/article/india-accuses-huawei-of-hacking-into-its-telecom-network/

63. Apuzzo, Matt, & Schmidt, Michael, "Secret Back Door in Some U.S. Phones Sent Data to China, Analysts Say,"The New York Times, November 15, 2016, https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html

64. Dalek, Jakub & ors. "A Chatty Squirrel: Privacy and Security Issues with UC Browser," The Citizen Lab, May 21, 2015, : https://citizenlab.ca/2015/05/a-chatty-squirrel-privacy-and-security-issues-with-uc-browser/

65. Brady, Anne-Marie, "China's Foreign Propaganda Machine,"Wilson Center: Kissinger Institute on China and the United States, October 26, 2015, https://www.wilsoncenter.org/article/chinas-foreign-propaganda-machine

66. Rawnsley, Gary, "Why China's Propagandists Love the Internet". Foreign Policy, July 21, 2015, http://foreignpolicy.com/2015/07/21/why-chinas-propagandists-love-the-internet/

67. King, Gary., Pan, Jennifer., & Roberts, Margaret, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument,"American Political Science Review, 2017, https://gking.harvard.edu/files/gking/files/50c.pdf

68. "UC Browser posing threat for security forces at border: MP Patel,". The Hitavada, April 12, 2017, http://thehitavada.com/Encyc/2017/4/12/UC-Browser-posing-threat-for-security-forces-at-border--MP-Patel.aspx

69. Mozur, Paul, "Alibaba Joins Forces With Chinese Arms Maker,"The New York Times, August 19, 2015, https://www.nytimes.com/2015/08/20/business/international/alibaba-and-weapons-maker-in-satellite-navigation-project.html

70 Buckley, Chris, & Perlez, Jane, "By Buying Hong Kong Paper, Alibabe Seeks to Polish China's Image,"The New York Times, December 13, 2015, https://www.nytimes.com/2015/12/14/world/asia/alibaba-south-china-morning-post-hong-kong.html

71. Timmons, Heather & Huang, Zheping, "Jack Ma is paying journalists "cash gifts" to stay at the newspaper he just took over," Quartz, April 7, 2016, https://qz.com/657604/jack-ma-is-paying-journalists-cash-gifts-to-stay-at-the-newspaper-he-just-took-over/

72. Reuters, "India silently countering Chinese influence on its telecom, power sector," Business Today, August 17, 2017, http://www.businesstoday.in/current/economy-politics/india-silently-countering-chinese-influence-on-its-sensitive-markets-china/story/258565.html

73. Aulakh, Gulveen, "India may force foreign handset makers to set up servers here to ensure data protection," The Economic Times, August 18, 2017, http://economictimes.indiatimes.com/articleshow/60110548.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

74. "Approval of National Policy on Electronics 2012," Press Information Bureau, October 25, 2012,http://pib.nic.in/newsite/mbErel.aspx?relid=88618

75. Rathee, Kiran, "Prasad promises new digital policies to make India $1-trn digital economy,". Business Standard, June 17, 2017, http://www.business-standard.com/article/economy-policy/prasad-promises-new-digital-policies-to-make-india-1-trn-digital-economy-117061600875_1.html.

76. "India-China bilateral trade relationship," Reserve Bank of India, August 7, 2014, https://rbi.org.in/scripts/PublicationsView.aspx?id=15010.

ORF OBSERVER RESEARCH FOUNDATION
Ideas · Forums · Leadership · Impact

20, Rouse Avenue Institutional Area, New Delhi - 110 002, INDIA
Ph. : +91-11-43520020, 30220020. Fax : +91-11-43520003, 23210773
E-mail: contactus@orfonline.org
Website: www.orfonline.org