Post Coronavirus World – Technology Imperatives: Make in India for self reliance

Dr Kamlesh Bajaj

The strategic nature of information and communication technology (ICT) products and services is not lost on any nation, since digital economy has contributed more to their national GDPs than any other sector. This is true both for the developed and developing countries. It has created more jobs as digitisation of businesses, e-commerce, banking, industrial work processes, education, health, agriculture, governance etc has increased. The rise of ever powerful computing platforms, machine learning (ML), and artificial intelligence (AI) using zillions of data bytes generated by ever increasing number of devices - Internet of Things (IoT) - connected to the Internet have speeded up the emergence of hyper-connected world. The basic Internet protocols to connect devices are universal, and products conform to international standards, though there is a race to control standards to the advantage of first movers – companies and nations. But ICT products designed and developed anywhere in the world, maybe produced in countries like China, Japan, Taiwan or South Korea, through global supply chains. This has resulted in the availability of products and services that are affordable. It has also led to efficient businesses and administrations, which deliver cost-effective services to consumers and citizens. Innovative applications, disruptive at times – like uber, zomato - have created new jobs of different kinds. Humans are learning to work with intelligent automated and robotised processes, both in industries and offices. They have to be re-skilled to stay relevant.

ICT is not only for economic growth and job creation, but also for gaining supremacy in cyberspace. The same Internet and products are of as much importance to militaries, if not more, to navigate and maintain their dominance for cyberattacks, surveillance and espionage, as in the civilian world for companies and governments. No wonder the race for technology supremacy in the digital global world has emerged as a key factor in defining the previous decade. While standards can be defined, algorithms maybe open, yet their implementation, such as for encryption, maybe controlled by companies. Vulnerabilities in products can be planted, or may get known later by discoveries made by users or hackers. The efficiencies brought about by global supply chains leave the issue of trust unresolved because the companies are in nations, which are in conflict; national laws can force their own companies to comply with for helping in surveillance of foreign citizens and governments when necessary. Many examples can be cited from both the western and communist worlds to support this.

Last few years have witnessed intense global debates for enhancing trust in global supply chains so that globalisation, inspired largely by the Internet, continues to increase economic activity in nations. Though nothing tangible has emerged in the United Nations, or in Track 2 diplomatic efforts led by think tanks, because the question of control, and trust in nations becomes paramount. Huawei and 5G rollout have become synonymous with this debate. Distrust by democratic countries like the US and India does not appear to be unfounded.

And now the coronavirus, Covid-19, originating from China, in over three months of breaking out in Wuhan, has almost the entire world under its deadly grip, with over 300,000 dead out of nearly three million infected by it, and still counting. With no cure, no preventive treatment, no vaccine in sight, locking down entire populations in cities, and countries, asking people to avoid physical contact with one another - which has come to be known as social distancing - is the only short-term solution to stop the cascading growth of infecting entire regions. As expected, this has brought large areas of economic activities to a grinding halt, resulting in unemployment, and affecting supplies of essential goods. For the first time in 60 years, Asia's growth will be zero! Indian economy has suffered tremendously, with its GDP growth projected to be zero or even negative. Both of these points have been discussed at length in several articles.

The focus of this paper is to examine the role of technology, globalisation, and trust in global supply chains by nations in times of such pandemics. Large sections of people, not only professionals working in ICT companies but other support staff too, have been asked to work from home. What are the lessons for India in economic security and national security? What is the criticality of technology – its use and indigenous development – keeping in view the global supply chains? Cyber security has been on top of the global agenda in engagements of think tanks, track 2, and multilateral fora. And now, in a quantum jump, corona with possibilities of bio-warfare, has left it way behind. However, since dependence on ICT has increased in this pandemic, ICT products and services, and their security are even more critical. Cyber is not disappearing anytime soon!

Pandemic shifts work online

Work from home (WFH) has suddenly strained the capacities of networks. E-commerce has emerged as an important channel to deliver groceries, food, medicines, and other services to citizens in lock down scenario. Government agencies rely on communication channels provided by messaging apps for coordination and effective action. If you add entertainment, education, and health sector, the scenario gets more intense. But then it is these technology platforms that are helping the society cope with the pandemic. E-commerce and social media – the messaging and video chatting – stand out for making life bearable for the locked down population. Entertainment via video streaming, and gaming are no less in keeping the people engaged. In short, it's the Internet with a handset, or a laptop, relying on high speed networks that form the core technology infrastructure for running numerous apps.

WFH using videoconferencing (VC) is a data intensive application. Multiple teams, each with several persons on VC platforms, require huge bandwidths. NYT reported on March 17, 2020 the challenges posed by working from home. Can the internet handle it? Reproduced in ET. (**https://economictimes.indiatimes.com/small-biz/startups/features/so-were-working-from-home-can-the-internet-handle-it/articleshow/74666280.cms**) WFH requires husband and wife (both working professionals) to be online for their respective VC calls and data sharing with their respective teams. The children, on the other hand, are busy watching streaming videos, using online gaming apps, and video calling their friends. Add to that the online school video lectures, assignments and exams. Perfect scenario for data explosion leading to frozen responses on home networks! In normal times, all these items are staggered, since parents are at work, and children at school. Video streaming and gaming are in the evening. But what the networks in cities like Palo Alto, Seattle and New York discovered that a bandwidth sufficient for a household with staggered use by its typically four occupants, could not cope with the WFH data requirement of all four! Europe reported increase of 70-80% traffic on WebEx, the VC service of Cisco. Italy reported spike on a local network by 80% because the children were on PC games from home during peak pandemic.
The data traffic has increased considerably. Many of the western countries, network operators have been requested to stop video-streaming of movies and other content in High Definition (HD) format,

restricting to Standard Definition (SD) only. Platforms like Netflix, Amazon, MX Player, and Hotstar hog huge bandwidths putting heavy load on the networks. School children are accessing teaching videos, lectures, assignments, exams online.

WFH has led to increase in data traffic in India. Almost entire IT/ITeS industry is working from home. It is not surprising that a surge of wired broadband data by 25-30% has been seen, since the lock down on March 25, 2020. (**https://telecom.economictimes.indiatimes.com/news/wired-broadband-data-surges-by-25-30-amid-lockdown-crisil/75404774).** There are more subscriptions for fixed broadband, especially in urban areas because of WFH. But this has led to slower speeds. India's fixed broadband, stagnating at 18-19 million connections since 2016, constitutes only 6% penetration compared with 55% in China, 70 in Europe, and 80% in Japan.

The Indian scene of ICT techies, with husband wife online for their respective VC calls and data sharing with their respective teams, is getting there; Covid-19 is accelerating that. Also, their children too have access to the same home WiFi network, and the Internet connection from a network provider (Airtel, Vodafone, Reliance Jio, BSNL). It's the same group which is accessing school lessons for 4-5 hours a day during lock down.

But one thing is clear. It's the digitisation of business, governance and social processes that has been taking place over the last decade or so, that has helped the society and economy cope with the pandemic in important ways. 4G networks that provide reliable and reasonable bandwidth, e-commerce platforms, messaging apps, Internet banking, digital payment systems, online food deliveries, online video consultation with doctors in hospitals, health monitoring devices, CCTV and drones for surveillance to monitor social distancing norms, and many more systems and apps have given confidence to the society that the basics for survival can be achieved through technology platforms.

The ICT products and services, till recently, have been around American platforms. Microsoft Windows, Office 365, Skype, Google search, Gmail, Google Docs, hosting; Social media apps like Facebook, WhatsApp, Instagram, Telegram; Clouds of Microsoft, Amazon, Google; Cloud computing platforms for AI and ML apps; IBM Watson; Amazon Web E-commerce platform; Cisco WebEx; Entertainment platforms like Netflix, Amazon; Encryption technologies, and many more. This is true of India, and most of non-Chinese world, though the picture is changing. With China pushing its hardware, and social media apps very quietly, over the years, we find ourselves submerged in their platforms!

ICT for the Education Challenge

The West is relatively well equipped to deliver education to school children and college students. Such platforms have existed there for 10-15 years. Most school children receive their assignments, grades online. Many schools have tied up with companies such as Google to deliver chrome-books to children for online teaching. These have proved handy in delivering all teaching material, video-lectures, assignments, exams to children online during usual school hours. The students miss the physical interactions with teachers and classmates, but during the lock down their studies have not suffered significantly in the US and Europe.

Quoting a UNESCO study, a Brookings paper states that as of April 14, 2020, 188 countries around the world have closed schools. Nearly 91% students, i.e. about 155 billion are affected. Less than 25% low-income countries are providing any remote learning – at best some TV and radio teaching. In contrast, 90% of high-income countries provide online learning opportunities. Upper-income countries, on the other hand – more than 70% of them – are providing a mix of online education with broadcast too. In the case of lower middle-income countries, nearly 66% are able to provide some form of online and broadcast education. But then in this category, only 36% of students have access to the Internet, which may not be of quality and speed that allows them to have online learning that can really be called as education. Among countries providing online education, 60% use online platforms, with nearly 35% distributing videos online. (School learning inequality around the world during COVID-19, Emiliana Vegas, April 14, 2020, Brookings)

The education apps, though small at present, are likely to pick up in a big way. As noted above, with all schools closed during this pandemic, it's the affluent group in India which is accessing school lessons and online content for 4-5 hours a day during lock down. And these kids are the ones who can access other education platforms, for additional proficiency in studies. But not the government schools. The lesson that emerges from this pandemic is that the existing divide between private and government schools, will become even greater in the form of digital divide. Unless addressed now, this will widen the gap further. Technology must be for all!

If the digital divide has to be bridged between the government and private schools, India will have to build teaching platforms with commensurate network capacities to cater to the requirements of staggering number of students.

Virtual classrooms in online universities are a reality in several western nations. They use Massive Open Online Courses (MOOC) platforms. These enable mature students to learn at their pace, at times convenient to them. This mode will have to be encouraged too to deliver the best subject lectures by expert teachers and communicators to wider audiences. Deficiencies and shortfalls in such experiments that have been conducted on a large scale by Indira Gandhi National Open University (IGNOU), using relatively primitive platforms, will have to be addressed through upgradation. Start-ups in India will have to be encouraged to develop projects with identified university partners to develop and deliver online content to anyone, anywhere. Private companies in education such as NIIT could be leveraged to help create platforms and desired content. We must remember that these should be developed by Indians, with large Indian funding to control the IPs, unlike some of the start-ups in this field with large external funding, which then end up being externally controlled.

ICT Security Challenges

This pandemic has shown that suddenly certain products come to occupy the centre stage. After the Chinese platforms Tik Tok, Help, Dailyhunt took over India in social media space – competing with the American Facebook, Instagram, Google News, Google hangout, Twitter in the Indian market –

Zoom is at the heart of WFH, and distant teaching classrooms, in India. Claimed to have been designed for enterprise users, Zoom has suddenly seen a surge in its use. It's the home users – those working from home during the pandemic – that have made it a heavily used app. Cornovirus has made Zoom the king of Quarantine Economy according to AdWeek, since with over 50 million downloads on Google Play Store by the end of March 2020, it displaced most popular apps like WhatsApp, Tik Tok, and Instagram in India. WhatsApp, despite its widespread use, slipped to fifth position. And reports at the end of April, put its users at 300 million! Zoom is free. Though Zoom Communications is incorporated in the US, like ByteDance owning Tik Tok, it is considered as Chinese owned.

Zoom gained prominence as a free platform that allowed 50 simultaneous users to be present in a VC. Although other platforms like Google hang out are free, and allow as many or even more users, it's Zoom that gained prominence for some reason. Among others, it is the ease of use that has increased its acceptance. There are other VC platforms, which are more secure, and are available to business users for a fee. But Zoom, nothwithstanding security and privacy concerns, which are numerous, continues to rule the roost. It has been found to be routing all calls and data through Chinese servers located in China. Even the encryption keys used for so called 'secure' communications are said to have been generated on servers in China. Zoom has admitted to these 'shortcomings'. Some of these probably can be addressed by using secure settings, just as in the corporate world WebEx, Google hangout and Meet allow users to do so. It is understood that even our Defence Minister used Zoom to VC with the Chiefs of Army, Air Force and Navy during the last few months. This resulted in an advisory being issued by the government. Incidentally, the US too noticed a spike in the usage of Zoom by Federal government employees, their children and others during the lock down period. A senator is bringing a bill to ban the use of Zoom on all government devices.

So, cyber security has to be integral to technology plans, more so in a pandemic, because, our reliance on technology in such times is significantly greater. Can Indian VC apps like Namaste and AirMeet succeed in the marketplace? Silicon Valley has responded aggressively to bring forth their VC products for greater use – Teams from Microsoft, Google Meet, WhatsApp VC, WebEx from Cisco. From being captives for corporate users, these platforms are now being promoted in the global market as teaching and conferencing tools by the schools and universities, and for governments. But then security of all these too will have to be ascertained through appropriate testing.

It may be noted that India has no general purpose apps – not even email (Rediff couldn't succeed). We present a huge market. It was only the US earlier; now China is gradually capturing the market with innovative apps. A nation that prided itself in software prowess stands deeply penetrated by huge Chinese apps – Tik Tok, Help (both from ByteDance), and now Zoom. Interestingly, ByteDance, headquartered in China, has registered as a company in the US. So has Zoom Communications. And many other multi-purpose apps tested extensively in China by the trio known as BAT (Baidu-Alibaba-TenCent) and others like taxi hailing app DiDi Chuxing, are at different stages of entry into India. They have invested in many start-ups with great potential. These companies invest not only directly, but through a number of their subsidiaries in Singapore, and Europe. It is well known that the Chinese government develops long range ICT plans, including Made in China 2025, in close concert with BAT and other private companies like Huawei, Xiaomi, China Telecom, China Mobile etc. China is using the Internet to power its economy, with a vision for Digital China. It is making huge investments, with private sector commitments and accountability for new products and services; their testing in its domestic market, and rolling out in the global markets with soft loans and funds from the government under Belt & Road Initiative. No wonder the world sees more and more of 'Made in China' ICT products and services.

Social Media Platforms

The importance of social media platforms during the ongoing pandemic hardly needs emphasising. AarogyaSetu piloted by NIC along with Google in India, has been tried earlier by its own app in China for effective control through tracing of infected persons, and for containment. Apple and Google are similarly tracking in the United States. These platforms are available in Europe as well. But while China uses its own apps on its own social media platforms, India does so on Google, WhatsApp, Apple etc. Their use by law-enforcement authorities (LEAs), health workers and medical doctors, NGOs, resident welfare associations, local authorities to spread the right message, control misinformation, coordinate for effective action in communities for contact tracing, has proved its use. That these are central to governance, during this pandemic, is not lost on anyone. Future pandemics or worse cyberwar kinetic outcomes may be much more challenging than Covid-19. Should India not have its own social media platforms, or remain dependent on those from the US or from China? The shape of such platforms maybe different; it can't be predicted except that the basic platforms will be equipped more and more with data analytics tools using AI and ML. Encryption technology will be an important component of this. India, a software powerhouse – can it accept the challenge? But then it's no longer merely a technology issue. It's a market challenge that requires government intervention to succeed.

Globally, the social media platforms have proved their utility in keeping the people engaged through videocalls, exchange of news and views, apart from their being used by LEAs, media, governments and NGOs for coordination and well being of people. So much so that media, civil society, law makers, and regulators which were calling for their regulation, privacy protection, antitrust suits to break their monopolies, are suddenly finding their use to fight the pandemic. Social distancing is being monitored through surveillance of smartphones. In the US, presidential campaign is almost being run on these platforms – it's nearly virtual. In Europe too, the regulators are quiet on privacy! Interestingly, these companies have responded by calling our fake news and rumours on coronavirus by ensuring that people are redirected to correct sites. That they can do so can have implications for privacy, data sharing for ad revenues for them, especially that these big global companies should work with governments to create data protection norms that are feasible. This will certainly have effect on the way society and governments view privacy, e-commerce, and surveillance, and much more.

Time to re-examine 'Make in India'. What are the achievements in hardware, networking, security products? Over 75% of mobile phone market has been captured by Xiaomi, Oppo, Vivo, Huawei, and OnePlus – all Chinese products. Laptops, servers too come from China. CCTV cameras, drones and surveillance technology also comes from China. So does the networking technology – base stations etc from Huawei and ZTE, both Chinese (also from Ericsson, Nokia and Samsung). And now social media and education apps too from China, in addition to those from the US!

It, however, needs to be reiterated that national security threats emanate from the US products too, and much has been written about that after Snowden revelations. But, given our geo-political situation, the threat scenario from China in ICT has to be viewed from a different lens – it is as bad as it can get. Doesn't require any deeper analysis for this piece; that is the job of defence, intelligence and foreign affairs. However, from cyber security angle, India must have Cyber Labs to test the products and services before these are launched here. Today, all the Big 4 consulting firms, all the big ICT services companies, and the telcos providing Internet services, have adequate capabilities for testing. Government needs to create an appropriate security testing ecosystem that can deliver.

Innovative apps from India like Dailyhunt have received high amount of funding from ByteDance, and other venture capital funds such as Japan's SoftBank, partly controlled by the Chinese. India's own first digital payment platform Paytm, also stands substantially funded by the Chinese. Many bigger start-ups in payments, mobility and e-commerce have received large amounts of funding from the Chinese companies. Chinese investors funded $4 billion into 90 start-ups last year. Alibaba and Tencent have funded into the following: BigBasket, DailyHunt, Paytm, and Paytm Mall, TicketNow, Snapdeal, Zomato, Byju, Ola, Flipkart, MXPlayer, Swiggy, Udan and many others. These have raised data security and platform control issues, as also propaganda and national narrative concerns. (Gateway House Report)

But the US companies' investments in Indian start-ups in security, AI, ML, encryption, and other innovative technologies and apps has not decreased. They are still the largest funders.

Technology Focus – ICT for India

It is against this background that I present the following **five important ICT areas for economic and national security. One** is the hardware for processing and storage of data with compute capabilities, adequate for the zillions of data bytes generated by apps and devices; used by AI and ML apps. The cloud data centres comprising servers with security devices and software. **Second** is the devices connected to the networks – mobile phones, smart IoT devices for industries and homes, CCTV cameras for security and surveillance, health monitoring devices – the so called end-user devices. Education platforms and apps. These are required in billions with varying degrees of capabilities. **Third** is that the underlying national networks should have huge bandwidths – 4G and even 5G networks – to connect all urban and rural areas with data speeds commensurate with their needs. Emerging apps requiring ultra reliability and low latency. Connecting the ubiquitous IoT devices for industrial apps. **Fourth** is the category of apps that drive the digital economy and empower individuals to engage in e-commerce, banking, payments, entertainment, video streaming, gaming, search, biometrics, facial recognition, email, instant chat messaging one-to-one or in groups, online education delivery tools, videoconferencing, tracking, surveillance, efficient and AI-based intelligent delivery of services in health including telemedicine, securing traffic for smart cities and agriculture. Sky is the limit as can be seen from the platforms and apps from Facebook, WhatsApp, Instagram, Google Search, Gmail, Twitter, Tik Tok, Dailyhunt, Zoom, and many more. **Fifth** is security of data, devices and infrastructure to protect individual's privacy, key national infrastructure, and national security. Economic security is the most critical part of national security, since direct physical kinetic attacks by adversaries are expensive with diminishing returns.

It's the cyber attacks on critical infrastructure to derail economies, steal personal data, economic data, intellectual property etc. are of concern to all nations. India is the most vulnerable to such attacks, what with all foreign ICT products and services, and apps with data stored outside India, that is 'secured' by foreign security products! Earlier the threat was only from the US and other powers from the West, since the ICT infrastructure and social media apps came from there; now much more so from China, since the PCs, laptops, mobile phones, 3G and 4G networks come from there. So, indigenous security products and services are key to enhancing security of our data – both at rest and in transit over communication networks. Foremost will be our capability and capacity to test these for security issues.

It is instructive to divide the national ICT infrastructure into broad categories to understand the productivity, innovation and security issues for the country for effective policy measures. Keeping in view the ever increasing importance of social media platforms for national and economic security, I have kept it as a separate category. These are as follows:

1. **The corporate systems and networks** operate Enterprise Resource Planning (ERP) systems, such as ORACLE or SAP on in-house hardware or in clouds. These systems are proven and in-use for decades for efficiently running corporate businesses, providing management support for decision making. Indian specialised platforms such as Core Banking software (TCS BaNCS, Infosys FINACLE etc) interface with ERP systems. More Fintech applications, using AI and ML, continue to emerge to address the ever increasing requirements of the BFSI (Banking and Financial Services Industry) sector as a vertical. Other important verticals include health, retail, governance, agriculture, network infrastructure, pharma, drug testing trials. Government systems like Aadhaar under UIDAI, GSTN and Customs under CBEC, Income Tax under CBDT, Immigration Control and many other areas require innovation in apps using data analytics tools.
2. **Basic hardware** – cloud servers, laptops, mobile phones; network devices like routers, switches; IoT devices.
3. **Productivity platforms and AI & ML Apps,** – e-commerce, payment systems, health, education, industrial apps, robotics, video-conferencing, video-streaming, smart cities, virtual and augmented reality;
4. **Security products and services, Testing Cyber Labs**: security products and services for securing cyber infrastructure, encryption, threat intelligence, cyber labs for testing products, services, and apps in the marketplace, etc.
5. **Social Media Apps** – chat, messaging, groups, entertainment, news, politics, elections; connecting individuals beyond the English speaking populations to all the local languages. (Local language Internet users will grow to 521 million, compared to 199 users in English – Google & KPMG Study, 2017)

The technology roadmap for India has to be drawn based on the five points and five categories, listed above; they create two different pictures of the same ICT products and services. Moreover, we need to understand the global supply chain challenges. An oft quoted example is that of the iPhone

6s which consists of 34 main components. Apple works with more than 200 suppliers in 43 countries on six continents to produce them. A single component has its own degree of complexity: the A12 chip designed by Apple in California is outsourced for fabrication to TSMC in Taiwan, is packaged and tested by Amkor in the Philippines, and then assembled into the iPhone by Foxconn in China or Pegatron in Taiwan. Back doors can possibly be inserted at many of these locations. The end product needs to be trusted by millions of users throughout the world. It carries the seal of Apple. Hence, **trust in the global supply chain is absolutely essential.** ("We traced what it takes to make an iPhone, from its initial design to the components and raw materials needed to make it a reality." https://www.cnbc.com/2018/12/13/inside-apple-iphone-where-parts-and-materials-come-from.html)

Security standards, open designs of products reviewed by experts, common criteria labs to vet the code, test and certify the process, and many other ways have been designed to certify products for global acceptance. But sadly, many instances of the products containing back doors installed deliberately, or left unwittingly because of poor design, misconfiguration, unknown Trojans are too well known; these are in the public domain. Despite several attempts, numerous examples of broken trust in the global supply chain are all too visible. While the US has been under scrutiny after Snowden revelations in 2013 when the National Security Agency (NSA) was found to be snooping on global citizens using backdoors in products and services provided by the American companies, it's China that is at the centre of similar concerns. Though it's the global manufacturer of most ICT products, it has lost trust in more ways than one. With its dominance of emerging 5G technology, AI and ML apps – latest being Zoom – the needle of suspicion from China is not going away anytime soon.

However, **if the global supply chain is not trusted, should one conclude that countries, including India, have to make their own technologies?** Not everyone can have their own chips, operating systems, semiconductors, encryption codes, search engines, social media, 5G phones/base stations/routers, cloud platforms and much more. But poles are likely to emerge – US and China – around which countries will have to gravitate. How long will it take? Dominance in 5G technology, and emerging social media apps from China might provide a clue, though western states are intervening to counter that by linking all to the Chinese Communist Party and the privacy law that requires vendors and operators to share data when demanded by the Chinese government.

While India will have to rely on underlying technologies from both the blocs, the need of times is to attempt to build some of the platforms itself by encouraging start-ups, and investing in R&D. With our market size, increasing Internet penetration, and focus on digital economy, this option has to be supported by government policies, at least in a few niche areas. **5G technology for secure networking is a key area in which indigenous technology developed by a network operator and start-ups should get state support immediately.**

Recommendations for the four categories listed above are as follows:

1. **Corporate sector** should continue to use global software platforms, and innovate in software using latest AI and ML tools to lead in the world. They have to conform to global standards, and be a part of the global system – banking, telecom, pharmaceuticals,

transport, retail and many more sectors. Innovating AI and ML apps using financial data, pharma data, telecom users data, weather data and so on. Design and develop our own security products and testing services. 5G, like 4G will need large scale testing of apps and services. All OTT services require ongoing testing for data security. Focus should be on development of security products in the country, and on developing testing capabilities in a series of cyber labs. Encryption products based on global standards developed indigenously for securing the transport layer are critical to national security.

2. **Hardware:** India has to move in a big way to manufacture servers, laptops, mobile phones, routers, and emerging IoT devices. Sheer volumes that are sold in India should be enough to inspire us. Why remain a perpetual importer of hardware for our data centres, cloud servers, routers and switches? This has to be led by the private sector. Government's role, however, is to facilitate key companies (American, Japanese, South Korean, Taiwanese) leaving China to move to India. Availability of land at viable rates, easy labour laws, and single window clearance for manufacturing units to get operational within 45 days. Such policies are essential – they have been talked about for long, but time to put them into practice is now.

   Likewise, policies for power availability to operate Data Centres, Clouds in India using hardware thus manufactured. Electricity for all is critical too if the digital divide between the rich and poor for accessing the Internet is to be bridged.

   Identify a few end-use products like mobile phones, laptops, routers, and IoT devices for large scale manufacture in India. Work with Samsung from South Korea, and with Japanese companies moving out of China to relocate in India. Encourage indigenous manufacturers too. This will give a stimulus to manufacturing components too. It can also lead to emergence of Android-like standard operating system in the country for mobile phones and IoT devices. It is important that this should be led by the private sector, with government supporting it by buying and deploying the hardware and software. We must remember that earlier attempts by the government in 1990s to create a Unix OS, based on open source Unix/Linux, did not succeed. It's not a one time effort. The OS has to be created, features added, and maintained by a company for continued use by the industry. This can't be done by a government agency. Android by Google is the latest example which makes it clear that Google has to expend large resources to keep it uptodate, and tailor it for new mobiles and IoT devices. A new model needs to be created that is led by the private sector.

3. **Productivity Platforms, innovative AI and ML Apps:** e-commerce, payment systems, health apps for monitoring and research, education platforms and their delivery mechanisms, industrial apps, GPS systems and apps, URLLC apps, surveillance and monitoring based on CCTV data, drones, facial recognition for law-enforcement agencies. Data generated by apps in India should be stored here, and made available in anonymised form to AI and ML developers for building apps for community usage, with adequate private ownership of IPRs and returns to the developers. No government interference in operations is the biggest incentive to start-ups. Regulatory approvals based on trusting the industry under a light touch, hands off environment is essential for growth. Privacy law, which is in making, should be a light touch regulation, based on universally accepted principles like data collection, purpose, processing, consent, retention. Data Protection Authority proposed under the law

should co-regulate, with industry as a partner, privacy and surveillance issues. Data sovereignty will be the automatic outcome of this.

4. **Security products and services, Cyber Test Labs:** enhance cyber security and protect data from unauthorised access. In the name of national security, extreme measures have been taken by nations that increase distrust in global supply chain. While these maybe a result of tensions for supremacy in cyberspace; developments in AI, ML, surveillance, encryption, 5G networking, semiconductors; or a trade war, these have made nations sit up and take notice. India cannot be and should not be immune to these developments. While some other technology points are covered in this paper, it's critical that we develop certain key security products, retain their IPRs, deploy them on large scale in the country. This industry is relatively young and small in size; mainly a greenfield for start-ups. It's the start-ups numbering around 175-200, with turnover of US$450 million (in financial year 2018) that are leading in pure play cyber products, data analytics, and remote security services, that are the backbone of this industry. Areas include antivirus, threat intelligence, identity and access control, IoT security, encryption, blockchain, and much more. They face significant challenges in getting their products certified and accepted by the government for wide use by the user industries. Innovation is the key here, and the young entrepreneurs are good at it, but the government support in testing and certifying their products and services is lacking. In the absence of capability within the government to test and certify products, users go along with foreign products with the stamp of Gartner or Forrester. This industry has the potential of reaching US$35 billion, employing 1 million persons, provided the right enablers are there to let the ecosystem develop.

   Cyber testing is an important area. India has capabilities in testing products and services for continued threats to critical infrastructure like banking, telecom, power generation and distribution, health care, surveillance and espionage, transport industry, retail sector, governance applications, social media platforms for creating unrest etc. Big 4 consulting firms, all the large ICT companies, telcos and banks have these capabilities. Cyber Labs exist within the infrastructure of these companies. These have to be leveraged in a coordinated way for giving a fillip to security in the country. CERT-In and NCIIPC need to play a proactive role in leveraging them.

5. **Social Media National Platforms:** Encourage development of national platforms for email, hosting, social media, business and home use apps like VC etc. China has done it by developing in-house replacements for search, facebook, twitter, amazon, uber etc) **No shame in starting even now, since these will rule the nations for all time to come, in ways that are unimaginable today.** This will reduce our dependence on either bloc. As a democracy, we can't isolate ourselves as a nation like China did by building firewall. But sadly, the private sector didn't pay enough attention to this. Rediff mail in the private sector didn't click. Nor did the government build a reliable email system for its secure use! Whole of India is using gmail, yahoo, and hotmail. We're the biggest users of WhatsApp and gmail and Facebook – much more than in the US where these platforms originated.

How can India break this jinx? Does NIC hold the key? Government needs to fund it as a project with NIC as the owner. Users will include: all employees of the central government, state governments, local governments, municipal offices; elected representatives at all levels. So, close to 15 million installed base is a big commercially viable project. If the present NIC Mail is not scalable, and doesn't have the features that are there in gmail and other mails, the new project should have all such features in the specs. The project should be developed by a private Indian IT company. This way India will have its own email system, that can be reliably used by all with whatever security features required; data will be stored in India. Encryption products conforming to international standards will be developed within India.

Perhaps government will have to force all departments, and state governments to use this platform. Over time, many of the public sector companies can also be made to shift to this platform. But there can be no compromise on the quality of service, features, storage, attachments and their size, utility etc. Operation of this email system should be contracted to the developer company – build operate model. As of today, it costs around Rs 1000 per user per annum as email fee to the company whose email package is being used by business – whether Gmail, or Microsoft or IBM. We're not talking about general population at large. That will come in the next phase.

Likewise, NIC can own a project for the development of secure messaging system like WhatsApp, for the 15 million users as for mail. End-to-end encryption will ensure secure messaging for government users, with data stored in India. But the government will have to get it developed by the private sector, which will also operate the system. In this pandemic, police, administration, citizen groups relying on Whatsapp.

The scale of these two projects can make a big impact on the country. Private mails can emerge to serve the needs of smaller companies and individuals with revenue driven by ad models, or for a small monthly fee. Messaging App can also become similarly available to the public for a nominal fee of a few rupees per month. These can be bundled by the mobile network operator in its fee. This maybe yet another approach to a private business model. Digital payments on such a local messaging system will be yet another attraction for users.

Start-up funding by the government doesn't seem to work. Some of the reasons are as follows: Start-ups require several rounds of funding to develop a product, add features, improve performance, change design along the way, get users to test beta-version, launch services. During this period the team expands, gets people for business growth, scaling up platforms and so on. Agility in approvals is the key. Funders, i.e. venture capitalists have to know the market. They use several channels to get market intelligence. They bring in management experts as CEOs to run the start up at some stage to expand business, while the developers focus on technology. Can government officials ever do that? Clearly not.

It is for this reason that the above project-mode has been proposed for email, and messaging platform. Once developed, these will be rolled out by the private sector and operated by them. NIC will be the owner, but not its operator; it will hold the private company accountable to the services contract. Government funds given for projects in this way are for public good, and will eventually help improve national security. Moreover, data will stay in India on Indian servers.

Other projects by the user ministries: Similar projects can be farmed out for development by start-ups and/or big companies to meet their specific requirements. For example, VC platform for MHRD. Improvements in biometrics authentication by UIDAI using AI and ML techniques. GSTN can plan projects for data analytics to track frauds. Income tax, Customs can create specs for similar projects using massive data, AI and ML algorithms. Health is another area. The key is flexibility to let smaller companies grow apps, with IPRs retained by them to go to global markets, after they have developed and implemented the user ministry requirements. Each ministry to create an ecosystem of developers around it to build apps. It must be flexible, and based on trust and usefulness. Creating initial specs for products and services required by a government agency holds the key to success of such a model. Whether CDAC may have a role here needs to be examined. But it can't become a boss which ends up stifling innovation.

Other innovative methods may also be used. For example, start-up VC platforms like Namaste and AirMeet, can be deployed immediately by an agreement such as Rs 100 or 200 per user per month. Use and help the vendor improve the product and service. But is it that simple? Success of Zoom during this pandemic has unleashed a war in the release of VC platforms that some of the big companies had reserved for the corporate users. Teams from Microsoft, Meet from Google, WebEx from Cisco. Google, with 100 million Meet users, has been made free – it will no longer require a business account to use. Google users will be able to download and use it for free with over 100 participants on a single server, for 60 minutes. Google's cloud unit that hosts Meet services does not send any ads to its business users; same policy will be followed for the free users as well. It will not record the videocalls of users. Business-only tool that is more secure and reliable modern product than its earlier free version Google hang out is suddenly available to normal users during corona. After October, calls beyond 60 minutes will not be allowed. Likewise Microsoft Skype, and Facebook Messenger have added more features for free use by general public. (**https://telecom.economictimes.indiatimes.com/news/google-makes-meet-video-conferencing-free-to-all-users-challenging-zoom/75448273**) These are secure platforms, which with proper security settings, can give confidence about secure videoconferencing. Google has assured that no VC usage of users will not be recorded by it. WhatsApp.

How does a country, with intent to build its social media platforms handle this arsenal that can be launched for free, by established players? Government has a role here. Incentives like buying products, giving minimum assured returns by using the platforms to help them establish, and grow.

However, general purpose apps like Helo and Tik Tok for fun, DailyHunt for news may be left to the market forces. But let's remember that they are capturing the Tier 2 and 3 cities in vernacular languages. Such apps will come and go – they may have short life spans, but they are likely to control the national narrative in many ways that can impact law and order, social discourse, and ultimately national security.

5G networks in India

Trials should include technology developed by start-ups. In consultation with major telcos – Airtel, Jio, Vodafone – 5G areas in cloud date centres, MEC, SDN and NFV, which are all software modules, be identified for R&D. India has expertise in software development. Start-ups and other private sector should be funded by the government, for testing and deployment by the telcos. But, the process of identifying challenge areas, and manner of funding start-ups and private sector be transparent, and easy, without government control. Telecom Industry will decide what products will be developed indigenously, with detailed specs, and identify companies which will develop; these will then be given to all the telcos for testing and deployment. Government will fund the effort, without dominating it. Liberal thinking about IPRs is essential. Indian telcos will use the products thus developed, but the developing companies should be free to sell them elsewhere in the world. We have to break the bureaucratic mindset in the government of owning IPRs. Government job is to get the technology developed by the private sector for indigenous use, and for enabling our industry go to the global marketplace. No monetary returns to be expected.

Indigenous 5G technology

Reliance Industries Limited (RIL) in its press release of 22 April 2020, on its partnership with Facebook emphasised the "world-class digital platform built by Jio, which is powered by leading technologies such as Broadband connectivity, Smart devices, Cloud and Edge Computing, Big Data Analytics, Artificial Intelligence, Internet of Things (IoT), Augmented and Mixed Reality and Blockchain." With a digital ecosystem comprising network, devices, applications, and content, Jio has emerged as a one stop shop for users for all kinds of services. It combines carriage, content and commerce. Through this partnership, it wants to help achieve 'Ease of Life' and 'Ease of doing Business' as part of its effort to contribute to PM Modi's 'Digital India' mission. (www.ril.com)

It is extremely heartening to learn that **Reliance Jio has developed the 5G platform indigenously.** It has developed end-to-end 5G technology – own hardware for 5G, and own Cloud-native platform. With its design, it can get the hardware manufactured by companies like Samsung, TSMC in Taiwan, and Japanese makers. It is actively building 5G and IoT technology capability in-house. The move is said to be unprecedented not only in India, but globally, since technology vendors are distinct from network operators. Samsung was its only vendor for 4G radio technology. Reliance Jio will be the only 4G and 5G network independent of Chinese technology – a first in India, and perhaps in the world. Jio plans to customize its technology based on 5G and IoT standards that will be adopted by India. It needs to be underlined that Jio's own IMS (IP Multimedia subsystem) solution (vIMS) for VoLTE and VoWiFi is live since October 2019. It was previously using Nokia's and Oracle's IMS, and related technology for 4G voice service. (https://economictimes.indiatimes.com/industry/telecom/telecom-news/reliance-jio-builds-in-house-5g-iot-replaces-nokia-oracle-tech-to-reduce-dependence-on-foreign-gear/articleshow/74541379.cms)

These indigenous 5G products and services, like any other from global competitors, should be tested by the government under the STQC Labs through accredited private labs under the Common Criteria plus 3GPP Standards, for functionality as well as for security. Some other start ups developing chips for specialised functions for 4G and 5G networks could be encouraged to integrate with the indigenously developed 5G network noted above. The government should encourage network operators to examine such technologies from a national security angle so that exposure to technologies from China for espionage may be minimised. The competitive issues can be handled separately.

Finally, India should take up the design and development of end-to-end holistic architecture of the national digital communications and computational infrastructure, that will act as a blue-print to decide the critical components that need to be controlled and regulated strategically, components can be supplied by global players, and components that need to be indigenously developed and deployed. It should also include encrypting the transport layer with our own encryption technology, so that irrespective of the underlying physical layer and 5G technology deployed from any vendor, our communications are secure. This guiding principle can help in policy decisions regarding the relevant technologies.

Conclusion

ICT infrastructure, products and services are critical to a nation's survival in pandemics, disasters, catastrophes, kinetic wars, cyber or biological wars. COVID19 has proved that. E-commerce and social media platforms, hundreds of apps riding on a reliable network infrastructure for health care, movement of essential goods and services; coordination between LEAs, health officials, citizen groups, NGOs and religious places providing cooked food to migrants and other working people – all have been made possible by the ICT infrastructure. WFH has been enabled by the same infrastructure. Online education to students during the pandemic too is taking place, thanks to technology platforms.

As expected, this experience has shown that the Internet savvy groups have access to all these services. But not those who don't have access to the Internet, or a reliable high speed network. Private schools delivering online education stand out in stark contrast to government schools. The digital divide couldn't be more striking! That this will lead to further divide in society, because of access to opportunities, is obvious.

Challenges of indigenous development of ICT platforms, social media, education, security have been discussed. India's extreme dependence on ICT from the US and from China has been discussed, and that India's economic and national security can be harmed in times of pandemics, and wars needs no elaboration. Some steps that need to be taken to build our own technology platforms, in certain areas, by promoting start-ups through testing, certification and acceptance of their products; promoting indigenously developed 5G technology, duly tested for conformance to global 5G standards. Reliance Jio 5G technology and special purpose chips developed by some of the start-ups must be tested for functionality and security. Being the only network in India (and perhaps in the world) that is not using Chinese technology, it deserves closer look by the government. Special focus should be on development, testing and use of indigenously developed security products and services, including encryption technologies. Cyber Labs with private companies for security testing must be leveraged.

Affordable access to the Internet, and to opportunities for education, health, news, entertainment, commerce, and business is the right of every citizen. Not only during pandemics and disaster, but even otherwise. For bridging the digital divide between the rich and poor, availability of electricity 24x7 to all sections of society is equally important. Cloud data centres too need 24x7 power at tariffs that make them viable. This will emergence of many more data centres that we require for data localisation in India.

(Dr. Kamlesh Bajaj was Founder Director, CERT-In, Ministry of Electronics and Information Technology. He was the Founder CEO, Data Security Council of India. He is a Distinguished Fellow, EastWest Institute, and an Honorary Advisor, PDPU, Gandhi Nagar. Views are personal)