Delhi Policy Group

DPG Cyber Review

Volume 1, Issue 3

APRIL 2020

Delhi Policy Group
Core 5A, 1st Floor, India Habitat Centre, Lodhi Road, New Delhi- 110003
www.delhipolicygroup.org

DPG Cyber Review
Volume 1, Issue 3
April 2020

ABOUT US

Founded in 1994, the Delhi Policy Group is among India's oldest independent think tanks with its primary focus on international and strategic issues of critical national interest. Over the past decades, the Delhi Policy Group has established itself in both domestic and international circles, particularly in the area of national security.

In keeping with India's increasing global profile as a leading power and the accompanying dynamism of India's foreign and security policy, the Delhi Policy Group has expanded its focus areas to include India's broader regional and global role; India's initiatives to strengthen its strategic periphery; India's political, security and connectivity challenges and policies across the Indo-Pacific; and the strategic partnerships that advance India's rise. To support these goals, the DPG undertakes research, publishes policy reports and organises conferences on strategic and geo-political, geo-economic, and defence and security issues.

DPG Cyber Review

DPG Cyber Review is compiled by our research team from publicly available information and open source media to provide an overview of significant developments related to cyber and digital technology domains during the month. Your comments and feedback can be addressed to Brig. Abhimanyu Ghosh (Retd.), Senior Fellow at abhi.ghosh@dpg.org.in

Cover Photographs:

1. *The Prime Minister, Shri Narendra Modi interacting with the Chief Ministers of states via video conferencing to discuss the emerging situation and plan ahead for tackling the COVID-19 pandemic, in New Delhi. Source: https://pib.gov.in/indexd.aspx*
2. *The Minister of State for Development of North Eastern Region (I/C), Prime Minister's Office, Personnel, Public Grievances & Pensions, Atomic Energy and Space, Dr. Jitendra Singh interacting with the former Army Generals and Air Marshals on COVID situation in J&K, Ladakh and NE Region through video-conferencing, in New Delhi on April 29, 2020. Source: https://pib.gov.in/PhotoCategories.aspx?MenuId=8.*
3. *Kerala Police experiments with cutting edge technology to simplify citizen services Source: Twitter @TheKeralaPolice*

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre,
Lodhi Road, New Delhi- 110003.
www.delhipolicygroup.org

DPG Cyber Review
Volume 1, Issue 3
April 2020

Contents

Abstract

The COVID-19 pandemic has brought out the importance of digital networks and service platforms like never before. Telecommunication networks that carry the internet to our homes, and the services that ride on those networks have become critical to economic activity and pandemic management. Most enterprises, educational institutions and healthcare providers have adopted video conferencing and digital meetings as the new normal. However, this has also attracted criminals and fraudsters for stealing credentials, disrupting services or demanding ransoms. Some nation states are said to have become active to obtain state secrets or research outcomes of coronavirus vaccines. Social media, meanwhile, has become the source of fake news and hate content which breeds disharmony in society.

Communication Technology driven contact tracing mobile application, Aarogya Setu, has become an effective tool in India's fight against Covid-19.

The recent business tie-up between two technology giants, Reliance Jio and Facebook, is a notable development which can enhance capability development, although both companies need to assuage concerns regarding privacy of data and net neutrality. Meanwhile, Airtel has entered into $1 Billion deal with Nokia to expand its 4G Networks.

Larsen & Toubro (L&T) has secured a major order from the Indian Army to manage, support and operate the military's ultramodern communications network, called the Armed Forces Network (AFN).

The pandemic has also brought to the fore the benefits of Blockchain technologies, which is being explored by NITI Ayog.

A task force of the Indian Ministry of Finance has reported that spectrum prices suggested by DOT are high and Telcos need to address slow data speed and lower penetration in rural areas.

Google and Apple have joined hands to deploy contact tracing technologies. Google is also planning an undersea cable 'Blue Raman' between India and Italy via Israel.

There have been instances of burning of 5G towers in European countries on the premise that 5G is the cause for the spread of the coronavirus. Both the WHO and the ITU have discounted such a linkage.

Samsung Electronics has pipped Huawei to become the top global 5G smartphone vendor in the first quarter of 2020. However, Huawei and ZTE have bagged 80% of 5G base station contracts in China covering 250,000 base stations in 28 regions.

On the technology front, China announced the trial of a state sponsored digital currency e-RMB in several cities. A sovereign digital currency provides a functional alternative to the dollar settlement system and blunts the impact of any sanctions or threats of exclusion both at a country and company level.

National Developments

Cyber Threat Scenario

On April 02, 2020, the Indian Computer Emergency Response Team (CERT-IN), the country's nodal cyber security agency, issued an Advisory that multiple vulnerabilities have been reported in the Zoom video conferencing application which could allow an attacker to gain elevated privileges or obtain sensitive information on the targeted system.[1] Again on April 15, 2020, CERT-IN issued an Advisory on Web Conferencing security, without naming Zoom. Various security issues cited by CERT-In include attackers joining the meeting uninvited; sending malicious links in chat to extract information; and shared content using third parties being stolen. CERT-IN has warned that these vulnerabilities, if not patched up on time, could allow attackers to exploit the target system and has prescribed best practices for using Web Conferencing.[2]

On April 12, 2020, the Cyber Coordination Centre of the Ministry of Home Affairs issued an Advisory on Secure use of the Zoom meeting platform by private individuals (not for use by government offices/officials for official purpose). It referred to earlier advisories of CERT-IN on the issue and issued necessary guidelines.[3]

On April 01, 2020, The Supreme Court directed the print, electronic and social media to maintain a strong sense of responsibility to ensure that unverified news capable of causing havoc is not disseminated. The Court noted that mass migration of large numbers of labourers was triggered by fake news that the lockdown would continue for about three months.[4]

On April 09, 2020, The Economic Times reported that the Maharashtra Cyber Police had noted a considerable increase in fake news, hate and communal content on social media. It had registered 132 cases till April 08, 2020, in this connection since the lockdown.[5] Maharashtra Cyber Police has also issued an advisory for Whatsapp groups and administrators.[6]

---

[1] CERT-In Advisory CIAD-2020-0011

[2] CERT-In Advisory CIAD-2020-0020

[3] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1615008 April 16, 2020

[4] file:///C:/Users/Delhi%20Policy%20Group/Downloads/PIB1609887.pdf

[5] https://timesofindia.indiatimes.com/city/mumbai/maharashtra-cyber-cell-register-132-firs-in-18-days-for-spreading-hate-fake-messages-on-social-media/articleshow/75054389.cms

[6] https://www.moneycontrol.com/news/trends/coronavirus-impact-maharashtra-cybercrime-officials-issue-advisory-for-whatsapp-groups-and-admins-5123401.html

Fake news and disinformation campaigns on social media targeting India from abroad continued unabated. On April 22, 2020, an anti-India tweet was posted by a twitter handle impersonating Oman's princess Mona bint Fahd al Said. A Pakistani ID @pak_fauj changed its name to Omani Royalty Mona bint Fahd al Said @SayyidaMona to spread propaganda and tweeted an anti-India rant threatening expulsion of Indian migrant workers. The Omani Princess Mona bint Fahd who was impersonated denied such posts and the Indian envoy to Oman thanked the Omani princes for this clarification. This was seen as an attempt of Pakistan ISI to sow seeds of discord between India and the Gulf nations using social media as a tool of war.[7]

On April 30, 2020, it was reported by ANI that the Indian Army has issued a warning to its personnel against Pakistani agencies' nefarious designs to hack the phones of Indian military personnel through a malicious application similar to the Aarogya Setu app. Inimical intelligence agencies have developed a malicious app by the name Aarogya Setu.apk. Such apps were found to be sent by Pakistani Intelligence Operatives to WhatsApp groups of Indian Army personnel. The Army has instructed its personnel that the Aarogya Setu application must be downloaded only from the Indian government website (mygov.in) or Android Play Store or iOS Apple Play Store.[8]

On April 29, 2020, the National Critical Information Infrastructure Protection Centre (NCIIPC) revealed that in view of the lockdown, several critical sector entities have relaxed their geofencing restrictions to allow their personnel to log-in and work from home. This has increased the attack surface available to threat actors (cyber criminals) from neighbouring countries. Sectors including government undertakings, strategic and public enterprises, banking and financial services, telecom, power, energy and transport, among others, are susceptible to such attacks. The NCIIPC under the NTRO has issued guidelines that include application whitelisting, blocking unused ports, turning off unused services and monitoring network traffic to prevent such attacks.[9]

On April 29, 2020, the Economic Times reported that Cybersecurity firms had alerted CERT-IN about conversations in the Darkweb linked to a Pakistan state-sponsored group that identifies itself as 'IOK', which could target India's health

[7] https://economictimes.indiatimes.com/news/politics-and-nation/fake-anti-india-tweet-on-behalf-of-omani-royalty-growing-trend-to-play-spoilsport-in-gulf/articleshow/75301807.cms

[8] https://www.hindustantimes.com/india-news/pakistani-spies-use-aarogyasetu-app-to-target-indian-military-personnel-army-issues-warning/story-cho7X9CK5ZqCA8un3OatrK.html

[9] https://telecom.economictimes.indiatimes.com/news/cyber-attack-fears-high-due-to-work-from-home-ntro/75440892

ministry and corporate donors to the PM Cares Fund. They also reported that a hacker group APT36 performs cyber-espionage operations with the intent of collecting sensitive information from India in support of Pakistani military and diplomatic interests. More than a dozen Pak government-backed attacker groups were using Covid-19 related themes as a lure for phishing and malware attempts, trying to get their targets to click malicious links and download files.

Recently, IT services firm Cognizant faced a Maze ransomware attack, which it said impacted clients as well.[10]

Digital Technologies

Communication Technologies

On April 02, 2020, The Government of India launched a mobile app "AarogyaSetu" for the health and well-being of every Indian in a resolute fight against Covid-19. This app has enabled people to assess themselves for the risk of catching the coronavirus infection by using their interaction with others, using Bluetooth technology, algorithms and artificial intelligence.[11] The Aarogya Setu app has recorded 75 million (7.5 crore) downloads till April 28, 2020.[12] A similar solution for feature phones is in the works and will be launched shortly.

On April 23, 2020, Facebook acquired a 9.99 % stake in Reliance Jio for INR. 43,547 Crore ($5.7 Billion). This is the largest FDI in India's technology sector thus far and could give a major boost to Indian Communication technologies. However, this deal will be closely scrutinized by privacy activists and anti-trust watchdogs as both companies have the private data of millions of Indians, which may give them undue advantage over rivals such as Google, Amazon or local start-ups.[13] Jio has emerged as India's largest telecom player with over 388 million subscribers within three years of its launch. Facebook has over 328 million users in India accessing its social network every month, while WhatsApp is present on over 400 million smartphones and is the most used messaging platform in the country.

[10] https://telecom.economictimes.indiatimes.com/news/increase-in-state-sponsored-cyber-security-attacks-on-government-bodies/75444846

[11] https://pib.gov.in/PressReleseDetail.aspx?PRID=1607490#

[12] https://telecom.economictimes.indiatimes.com/news/after-aarogya-setu-app-similar-solution-for-feature-phones-in-the-works-to-be-launched-soon/75430395

[13] https://economictimes.indiatimes.com/tech/internet/facebook-buys-9-99-stake-in-reliance-jio-for-5-7-billion/articleshow/75283735.cms

However, on April 27, 2020, the Policy think tank Broadband India Forum (BIF) dismissed the concerns around net neutrality and data sharing resulting out of the Jio Platforms-Facebook deal as "erroneous, farfetched and not based on facts". The group which counts both Jio and Facebook as its members, said that it is deeply committed to the cause of 'Broadband for All', involving the principles of liberalisation and competition, as well as scrupulous adherence to the regulations as regards Net Neutrality, Data Protection, etc.[14]

On April 28, 2020, it was reported that the Finnish telecom gear maker Nokia will deploy around 300,000 radio units for Bharti Airtel by 2022 under the newly reconstructed multi-year deal valued at around $1 billion to allow the telco to significantly expand its 4G network and to lay the foundation for high-speed 5G technology.[15]

5G Technology

The 5G spectrum auction is likely to be delayed in India amid the Covid-19 crisis. It was reported on April 06, 2020 that the government is unlikely to hold a 5G spectrum auction in June. The earliest possible date for 5G rollout is likely to be 2021-22, with a possible auction in October-December this year.[16]

Blockchain Technology

Covid-19 has brought out the challenges to ensure 'supply chain visibility' practices for essential goods. On April 24, 2020 it was reported that NITI Aayog is exploring the potential of applying blockchain in the case of a pilot project on pharmaceutical supply chains. Earlier in January, 2020 NITI Aayog, in its discussion paper 'Blockchain: The India Strategy', had posited that blockchain technology could offer a technological means for meeting supply chain challenges. The blockchain platform lends itself to ensuring quality assurance through tracking the supply chain and compliance with norms for transportation and storage with minimal manual intervention. Onboarding various tiers of suppliers of various supply chains onto a common blockchain platform would thus enable businesses and government to form a data driven view of their supply chains, and help minimise disruption caused by future disasters.[17]

---

[14] ET Telecom April 27, 2020.

[15] https://telecom.economictimes.indiatimes.com/news/1-bn-deal-nokia-to-deploy-3-lakh-radio-units-for-airtel-by-2022/75422777

[16] https://www.telegraphindia.com/business/coronavirus-lockdown-delays-5g-auction/cid/1762331

[17] https://www-livemint-com.cdn.ampproject.org

Government Initiatives

Strategy/ Policy/Regulation

Telcos and technology companies have urged the telecom department (DOT) and the electronics & IT ministry (MeitY) on April 28, 2020 to expedite steps to consolidate the over 40 Covid-19-tracker government apps under Aarogya Setu to reduce bandwidth usage and sharpen the pandemic tracking process. In a recent presentation to DoT and MeitY, telcos also called on the government to facilitate installation of in-building broadband gear such as distributed antennae systems (DAS) and small cells across gated communities to boost fibre-to-the-home (FTTH) connectivity, as vast swathes of people are likely to continue working from home for a prolonged period with no early end to the Covid-19 pandemic in sight.[18]

Budgetary Support

In a report released on April 30, 2020 a task force constituted by the Finance Ministry stated that the 5G spectrum price suggested by the Department of Telecom is too high, particularly as it recommended rationalising of prices for making the next generation services affordable for all. The task force acknowledged stress in the telecom sector and said the Supreme Court judgement mandating companies to pay around Rs 1.35 lakh crore ($17.86 Billion) has placed some operators in a "precarious position" due to the short period of time in which they have to meet their liabilities. The report also noted that lower penetration of digital infrastructure in rural areas and slow data speeds have restricted the full potential of digital technologies such as Internet of Things, cloud computing and artificial intelligence and recommended measures to address these issues.[19]

On April 14, 2020 the Ministry of Electronics and Information Technology (MeitY) announced an "Innovation Challenge for Video Conferencing Solution". The 'Challenge' has been launched to provide indigenous alternatives to address security and privacy issues of global Video Conference platforms. This will be conducted in three stages. Ten teams with innovative and cutting-edge solutions will be selected in stage1 and provided a funding of Rs 5 lakh ($6606) each to build the prototype. In stage 2 the top three selected teams will receive Rs 20 lakhs ($26429) each to build the solution. In the final

[18] https://telecom.economictimes.indiatimes.com/news/consolidate-covid-19-tracker-apps-to-reduce-bandwidth-usage-telcos/75462630

[19] https://telecom.economictimes.indiatimes.com/news/5g-spectrum-price-suggested-by-dot-too-high-finance-ministry-task-force/75479050

stage, the winner will receive Rs 1 crore ($ 1.32 Million) and a certificate from the Minister of Electronics and IT towards deploying the solution for use by Government of India and State Governments for a year and further support at Rs 10 lakhs($13223) per year towards operations and maintenance, for a period of three years. Participants can be from industry and academia, and the participating teams need not necessarily be registered Indian companies or startups. However, the teams selected at Stage 1 will then have to register themselves as Indian startups or companies.[20]

Capability Building

It was reported on April 18, 2020 that Larsen & Toubro (L&T) has secured a major order from the Indian Army to establish a first-of-its-kind, state-of-the-art Unified Network Management System (UNMS) to manage, support and operate the military's ultramodern communications network, called the Armed Forces Network (AFN), covering 60,000 Kms of Optical Fibre network built by BSNL. This will enable the Indian Army, Navy and Air Force's 414 bases across the country to communicate and exchange data securely. The company, which won the Rs 2,700 crore order, is required to discharge it within 18 months. At the heart of L&T's UNMS software system is the Next Generation Operation Support System (NGOSS), which will give complete visibility and real-time monitoring of the diverse network assets on a common management platform. Given the military's requirement for watertight cyber and communications security, L&T will establish a "Security Operations Centre" at a centralised location, which will deal with security threats, logs, alerts, archives etc.[21]

[20] https://www.dqindia.com/meity-announces-innovation-challenge-video-conferencing-solution-winner-get-rs-1-crore/

[21] https://www.business-standard.com/article/article_id=120041801269_1/Ajai Shukla

International Developments

Cyber Space

The World Health Organization has been in the news not only for its inept handling of the COVID-19 pandemic. However, but also for cyber-attacks against it. On April 02, 2020 Iran was accused of attempting to hack into the personal email accounts of the staff at World Health Organization. The attempted cyber-attack appears to have failed, but according to Reuters it had links with the Iranian regime.[22]

On April 22, 2020 Google warned that nation-backed hackers are exploiting the coronavirus pandemic to target health care organizations and those working to fight the pandemic. It has identified more than a dozen state-sponsored groups using COVID-19 themes as bait in phishing and malware traps. US and British security agencies issued similar warnings, saying some 2,500 web addresses were linked to various fraud schemes. Google reported that it was detecting about 18 million pandemic-themed malware or phishing messages per day and 240 million COVID-linked spam messages.[23]

On April 18, 2020, US Secretary of State Mike Pompeo called upon all states not to turn a blind eye to criminal activity against Health Institutions from their territory. He added that he was concerned by 'malicious' cyber-attacks that have targeted Czech hospitals battling the novel coronavirus, vowing "zero tolerance" for such attacks. The Czech National Cyber and Information Security Agency NUKIB on Thursday warned against attacks to its Hospitals in the eastern Czech cities of Olomouc and Ostrava. The Czech Republic is an EU and NATO member state of 10.7 million people.[24]

The Cyber Security firm, Fireeye reported on April 22, 2020 that from at least January to April, 2020 suspected Vietnamese actors APT32 carried out intrusion campaigns against Chinese targets designed to collect intelligence on the COVID-19 crisis. Spear phishing messages were sent by the actor to China's Ministry of Emergency Management as well as the government of Wuhan province, where COVID-19 was first identified. This incident, and other publicly reported intrusions, are part of a global increase in cyber espionage related to the crisis, carried out by states desperately seeking solutions and

[22] https://www.telegraph.co.uk/news/2020/04/02/iran-accused-attempting-cyber-attack-world-health-organisation/

[23] https://www.securityweek.com/nation-backed-hackers-tune-attacks-covid-19-fears-google April 22, 2020

[24] By AFP on April 20, 2020

non-public information.[25] Vietnam Foreign Ministry spokesperson, however, said that the accusation is baseless and Vietnam forbids all cyber-attacks, which should be denounced and strictly dealt with by law. [26]

On April 30, 2020 the BBC quoted a senior US intelligence official saying that the US has seen foreign spy agencies carry out reconnaissance of research into a coronavirus vaccine. In mid-April, an FBI official said there had been "some intrusions" into institutions working on Covid-related research. Bio-medical data had long been a priority target for cyber-espionage and organisations publicly linked to work on the virus had become targets.[27]

On April 30, 2020 Security Week magazine revealed that several water and wastewater facilities across Israel were targeted in a coordinated attack on April 24 and 25, 2020. The attacks targeted wastewater treatment plants, pumping stations and sewage facilities. Israeli Authorities said the threat actors targeted programmable logic controllers (PLCs) used to control valves, but that they did not manage to cause any damage. Organisations in the water sector have been instructed by Israeli authorities to immediately take measures to prevent attacks, including changing passwords to internet-exposed control systems, reducing internet exposure, and ensuring that all software is up to date. SCADAfence, an Israel-based OT and IoT security company, told Security Week that the attacks may have originated from the Gaza region and they might have been launched by an anti-Israel hacktivist group calling itself the Jerusalem Electronic Army.[28]

Spending more time on virtual platforms can leave children vulnerable to online sexual exploitation and grooming. The UNICEF on April 14, 2020 warned that children are at increased risk of harm online during the COVID-19 pandemic. More than 1.5 billion children and young people have been affected by school and college closures worldwide. As a result, these students are now taking online classes as well as socialising more on the internet.[29] Adequate measures need to be taken for the online safety of children and young people.

Digital Technologies

[25] https://www.fireeye.com/blog/threat-research/2020/04/apt32-targeting-chinese-government-in-covid-19-related-espionage.html

[26] https://telecom.economictimes.indiatimes.com/news/increase-in-state-sponsored-cyber-security-attacks-on-government-bodies/75444846

[27] https://www.bbc.co.uk/news/technology-52490432

[28] https://www.securityweek.com/hackers-knew-how-target-plcs-israel-water-facility-attacks-sources

[29] https://news.un.org/en/story/2020/04/1061742

Communication Technologies

On April 10, 2020 Apple and Google announced a partnership on COVID-19 contact tracing technology. Both organisations through a joint initiative will enable the use of Bluetooth technology to help governments and health agencies reduce the spread of coronavirus, with user privacy and security central to the design.[30]

On April 10, 2020 the US Department of Justice along with several other federal agencies requested the Federal Communications Commission (FCC) to terminate China Telecom's authorisation to operate in the U.S. They contended that China Telecom is vulnerable to exploitation, influence, and control by the Chinese government.[31]

Google is expanding its global cyber optics network. On April 14, 2020 the Israeli newspaper Haaretz reported that Google is planning a cable called 'Blue-Raman' (named after the Indian Noble Prize Winner Venkata Raman) that will run between India and Italy through Israel. The estimated cost of this project is $400 million. The Raman half of the cable will start in Mumbai, run beneath the Indian Ocean and overland across an unnamed country (presumed to be Saudi Arabia), before ending at the Jordanian port of Aqaba.[32]

Artificial Intelligence

On April 27, 2020 the Royal United Services Institute (RUSI) published a report that UK intelligence Agencies will need to use artificial intelligence (AI) to counter a range of threats from adversaries who are likely to use the technology for attacks in cyberspace and on the political system. RUSI also argues that the use of AI could give rise to privacy and human-rights considerations, which will require new guidance. The independent report was commissioned by the UK's GCHQ security service and had access to much of the country's intelligence community.[33]

[30] https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/

[31] https://www.justice.gov/opa/pr/executive-branch-agencies-recommend-fcc-revoke-and-terminate-china-telecom-s-authorizations

[32] https://www.haaretz.com/israel-news/business/.premium-israel-to-play-key-role-in-giant-google-fiber-optic-cable-project-1.8764470

[33] https://www.bbc.com/news/technology-52415775

5G Technologies

A UN News report on April 24, 2020 stated that since the COVID-19 pandemic spread across the world almost four months ago, 5G phone masts have reportedly been damaged or destroyed in several European countries, including Ireland, Cyprus and Belgium. In the UK, dozens of towers were targeted and engineers abused on the job. The scale of the problem prompted the World Health Organisation (WHO) to clarify that viruses cannot travel on radio waves/mobile networks. COVID-19 is spreading in many countries that do not have 5G mobile networks.[34] Earlier, the International Telecommunication Union (ITU) had stated that there is no scientific basis to link 5G and Covid-19. Bringing trusted news and facts about Covid-19 is of paramount importance.[35]

On April 22, 2020 Britain's permanent undersecretary and head of the diplomatic service at the foreign ministry stated that the UK Government has made a firm decision to allow Huawei into non-sensitive parts of its 5G network, capping its involvement at 35%, and this matter is not being reopened. He further stated that China is a very important partner of the United Kingdom and it is compatible to proceed with the Huawei decision and have a strategically independent relationship.[36]

On April 30, 2020 it was reported by IANS that Samsung Electronics has pipped Huawei to become the top 5G smartphones vendor in the world in the first quarter of 2020. Global 5G smartphone shipments grew to 24.1 million in Q1 2020, significantly more than the 18.7 million 5G smartphones shipped in the full year in 2019. China is the leader in demand for 5G smartphones.[37] However, Samsung Electronics Co has warned of a significant drop in mobile earnings in the second quarter, as recession following the COVID-19 pandemic may delay the rollouts of fast 5G networks in advanced markets like Europe and the United States. In China, it expects a boost in 5G spending due to government stimulus measures, but analysts say the policies will benefit local rivals such as Huawei Technologies and Xiaomi Corp more.[38]

---

[34] ET Telecom April 24, 2020

[35] https://www.itu.int/en/Pages/COVID-19/5g-covid-19-statement.aspx

[36] https://telecom.economictimes.indiatimes.com/news/uk-made-a-firm-decision-on-huawei-in-5g-foreign-ministrys-top-official/75284339 22 Apr

[37] https://telecom.economictimes.indiatimes.com/news/samsung-beats-huawei-in-q1-global-5g-smartphone-battle/75472186

[38] https://telecom.economictimes.indiatimes.com/news/samsungs-phone-fortunes-wane-as-covid-19-hits-5g-phones-in-europe-and-u-s-/75463202

On April 27, 2020 it was reported that Chinese vendors Huawei and ZTE have secured the bulk of a contract to provide up to 250,000 5G base stations to China Telecom and China Unicom. With these new contracts, the two Chinese vendors have already secured more than 80% of China's 5G base station contracts. According to local press reports, Huawei won 57.3% of the value of contracts across 28 provinces, with ZTE taking 28.7%, Ericsson 11.5% and China Information Communication Technologies 2.6%. In the new phase of its 5G program, China Mobile is aiming to acquire over 232,000 5G base stations as it looks to extend coverage to 28 regions across China.[39]

Block Chain Technologies

China has a grand strategy to lead the digital transformation of the world economy. As part of this, China is about to launch its national Blockchain platform internationally. On April 20, 2020, Asia Times citing Cointelegraph reported that the Blockchain Service Network (BSN) was poised to launch globally on April 25, 2020. This evoked the "Made in China 2025" initiative to spearhead innovation in areas such as robotics and artificial intelligence.[40]

On April 28, 2020 the paper Guardian reported that China has started major trials of a state-run digital currency the e-RMB in several cities, including Shenzhen, Suzhou and Chengdu, as well as a new area that will host some of the events for the 2022 Beijing Winter Olympics. A sovereign digital currency provides a functional alternative to the dollar settlement system and blunts the impact of any sanctions or threats of exclusion both at country and company levels. It may also facilitate integration into globally traded currency markets with a reduced risk of politically inspired disruption.[41]

[39] https://www.rcrwireless.com/20200427/5g/huawei-zte-already-secured-over-80-china-5g-contracts-

[40] https://asiatimes.com/2020/04/china-set-to-launch-global-blockchain-initiative/

[41] https://www.theguardian.com/world/2020/apr/28/china-starts-major-trial-of-state-run-digital-currency

Multilateral Cooperation

On April 27, 2020 the International Telecommunication Union (ITU) and the Ministry of Information and Communications, Vietnam announced that due to the COVID-19 pandemic, they have postponed ITU Digital World 2020, the global tech event for government, industry and SMEs. The event will now take place as ITU Digital World 2021 in September, 2021 in the same venue in Ha Noi, Vietnam.[42]

[42] https://www.itu.int/en/mediacentre/Pages/STMNT02-2020-Postponement-of-ITU-Digital-World.aspx

Delhi Policy Group
Core 5A, 1st Floor,
India Habitat Centre, Lodhi Road
New Delhi - 110003
India

www.delhipolicygroup.org