Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

JANUARY 2021

Volume II, Issue 1 | January 2021

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

Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG Cyber Review
Vol. 2, Issue 1
January 2021

ABOUT US

Founded in 1994, the Delhi Policy Group (DPG) is among India's oldest think tanks with its primary focus on strategic and international issues of critical national interest. DPG is a non-partisan institution and is independently funded by a non-profit Trust. Over past decades, DPG has established itself in both domestic and international circles and is widely recognised today among the top security think tanks of India and of Asia's major powers.

Since 2016, in keeping with India's increasing global profile, DPG has expanded its focus areas to include India's regional and global role and its policies in the Indo-Pacific. In a realist environment, DPG remains mindful of the need to align India's ambitions with matching strategies and capabilities, from diplomatic initiatives to security policy and military modernisation.

At a time of disruptive change in the global order, DPG aims to deliver research based, relevant, reliable and realist policy perspectives to an actively engaged public, both at home and abroad. DPG is deeply committed to the growth of India's national power and purpose, the security and prosperity of the people of India and India's contributions to the global public good. We remain firmly anchored within these foundational principles which have defined DPG since its inception.

DPG Cyber Review

DPG Cyber Review is compiled by Brig. Abhimanyu Ghosh (Retd.), Senior Fellow for Cyber Security and Digital Technologies 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. He can be reached at abhi.ghosh@dpg.org.in.

Cover Photograph:

World digital map

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

DPG Cyber Review
Vol. 2, Issue 1
January 2021

Contents

Abstract

In terms of Indian policy, there were several important developments related to digital technology in 2020, including the banning of more than 200 applications, the promulgation of the National Telecom Security Directive, and controls on FDI policy on grounds of national security. The National Cyber Security Strategy, the Draft Personal Data Protection Bill and the draft Non-Personal Data Framework remained under active discussion for implementation in 2021.

Data privacy issues came to the fore in January, triggered by the notification of a privacy policy update by WhatsApp. Implementation of this update was postponed from February 8 to May 15, following the exodus of a significant number of 400 million Indian WhatsApp users to rival messaging platforms like Signal and Telegram. This problem can be addressed only by the early adoption of a law on data privacy and security in India.

While common netizens were perturbed by privacy concerns, security agencies were challenged by innovative apps capable of encrypted communication on 2G networks and virtual SIM cards used by terrorist organisations in Jammu and Kashmir. Meanwhile, ransomware and phishing attacks remained the preferred mode of cybercrimes in the national cyber space.

Indian telecom service providers are gearing up for an early roll out of 5G, while the government is facilitating them with commercially viable policies and spectrum availability.

Global cyber scene during the month was dominated by the role played by digital corporations and the technologies that facilitated the Capitol siege on January 6 and legal investigations thereafter.

The US investigation into the SolarWinds hack, reported last month, remained under progress.

Semiconductor chips have become strategic assets in the ongoing geopolitical contest and China presently find itself decoupled from its global supply chain. TSMC's chip-making skills have handed Taiwan political and economic leverage amidst the US-China technology standoff.

National Developments

Cyber Threat Scenario

The national cyber space has been dominated this month by privacy concerns triggered by a policy update by WhatsApp on January 4, which notified users in India to accept sharing of data with its parent company Facebook or see their accounts removed from February 8. The new policy presumably targets business interactions, transactions and other business-related features, which will allow WhatsApp and Facebook to support third-party service providers. There is no option for users to opt out. This has raised a huge concern regarding privacy in India and a significant number of the 400 million Indian users of WhatsApp have migrated to rival messaging platforms, Telegram and Signal. WhatsApp has now decided to delay implementation of this policy till May 15, 2021.

What is intriguing is that WhatsApp follows different norms for users in Europe, because the EU has a strong General Data Protection Regulation (GDPR) that treats the safety of its users' data diligently and seriously.[1] This regionally differential treatment has prompted the Ministry of Electronics and IT to ask WhatsApp to respond to a series of 14 questions. In its submission before the Delhi High Court, on a Public Interest Litigation (PIL) on violation of privacy by WhatsApp, the Indian government on January 25 also raised the issue of WhatsApp following differential norms on privacy for its users in India and in Europe.

Migrating to alternate messaging platforms for better security and privacy is, however, illusory. Both Signal and Telegram are registered abroad and have their own issues. Signal is entirely Cloud based, which puts data at risk. The company was started in 2018 with a $50 million loan by WhatsApp founder Brian Acton as a non-profit platform and is popular among activists and dissidents. On January 26, a former engineer of Signal expressed concern that an explosion in growth - prompted by users moving over from rival WhatsApp - could cause extremism to spread on the platform. Telegram does not store data within the boundaries of India. Its development team had to leave Russia

[1] https://telecom.economictimes.indiatimes.com/news/telegram-or-signal-welcome-to-the-illusion-called-data-security/80312784

due to local IT regulations and is based in Dubai.[2] The remedy lies in the early implementation of a dedicated law on data privacy and security in India.[3]

The draft Personal Data Protection Bill, 2019 (PDP Bill, 2019) is under consideration by the Joint Parliamentary Committee and is likely to be tabled in Parliament during the current budget session. The bill is firmly grounded on the notion of informed consent and purpose limitation for data collected and stored. This needs to be legislated soon to prevent unilateral action by a commercial enterprise.

While privacy of personal data is sacrosanct, the business requirement to harvest non-personal data for targeted advertising and innovations is also a necessity. There is a need to incentivise consent for the consumer, from whom the data is harvested. Recognising the need to work out the framework for sharing of non-personal and anonymised personal data, the Indian government had constituted a multi-stakeholder Committee under the chairmanship of an industry veteran, Shri. Kris Gopalakrishnan, in 2019. This Committee published its first report in September 2020 for public consultation. Comments on the revised draft report have been invited by January 31, 2021. The committee, while recommending a data sharing framework for generating economic benefits, has raised concerns of data lock-in by monopolies. This process also needs to be fast tracked to preserve privacy and yet help economic growth aided by artificial intelligence.[4]

Attacks on Indian Cyberspace

While common netizens remained perturbed with the privacy concerns, terrorist organisations in Jammu and Kashmir and their handlers from Pakistan have shunned WhatsApp and Facebook Messenger for alternative platforms, including one developed by a Turkish company. As reported on January 24, security agencies have unearthed these applications which have the ability for encrypted communication with 2G internet services and overcome the ban on high-speed mobile data services in J & K till February 6. This comes at a time when security agencies in the Kashmir valley are also

[2] https://www.businessinsider.in/tech/news/as-signal-downloads-surge-employees-are-reportedly-worried-the-messaging-app-isnt-doing-enough-to-head-off-extremism
[3] https://www.businesstoday.in/technology/news/pil-against-whatsapp-new-privacy-policy-in-delhi-hc-says-violates-fundamental-rights/story/427986.html
[4] https://telecom.economictimes.indiatimes.com/news/as-privacy-becomes-a-hot-topic-this-weeks-debate-centres-around-the-data-protection-bill-will-it-do-enough-to-protect-your-digital-data/80323302

fighting the menace of virtual SIM cards, which have been in operation since the Pulwama attack on the CRPF convoy in 2019.[5]

On January 7, it was reported that about 3.5 crore records with masked card data and card fingerprint of the digital payments gateway Just Pay were compromised by the hacker named 'Shiny Hunters'. The report added that 10 million user databases belonging to three more Indian companies were on sale on the Dark Web.[6] In yet another data breach, reported on January 21, sensitive data of nearly 3.25 lakh users of India-based global cryptocurrency exchange and wallet, BuyUcoin, were exposed on the Dark Web.[7] According to the cybersecurity firm Coveware, the average ransomware payout has grown from less than $10,000 per event in 2018 to more than $233,000 per event in 2020.

Ban on Chinese Apps to remain

On January 27, the Chinese Embassy opposed India's decision to make permanent a ban imposed on Tik Tok and 58 other Chinese apps in June 2020, calling it discriminatory and in violation of WTO rules. The order to make the ban permanent had been issued by the Indian government after reviewing the replies of companies which owned apps blocked under section 69A of the Information Technology Act for activities which are prejudicial to the sovereignty and integrity of India, defence of India, security of the state and public order.[8]

Roll out of 5G Communications

On January 27, Airtel demonstrated its readiness to field 5G. Using dynamic spectrum sharing, Airtel seamlessly operated 5G and 4G concurrently within the 1800 MHz band spectrum block. Further, under its Make in India strategy, Airtel is planning to bring a large ecosystem of partners including US's Mavenir, Xilinx and Altiostar, Japan's NEC and Taiwan's Sercom that will help the telecom operator to develop equipment using Open Radio Access Network technology. Airtel is already partnering with Ericsson and Nokia to supply 5G radio equipment from India based plants. These announcements by Airtel and

[5] https://timesofindia.indiatimes.com/india/terror-groups-in-pakistan-switch-to-new-messaging-apps/articleshow/80433381.cms
[6] https://cio.economictimes.indiatimes.com/news/digital-security/3-more-indian-firms-hacked-data-of-over-10-million-users-up-for-sale-on-the-dark-web/80148941
[7] IANS January 21, 2021
[8] https://www.aninews.in/news/world/asia/china-opposes-indias-decision-to-continue-chinese-apps-ban-says-it-violates-wto-rules20210127163147/

earlier by Reliance Jio to field their own 5G technology are positive indicators for early roll out of 5G in India.

Allocation of Spectrum

The government on its part has eased the path for 5G rollout by reducing to six months the notice period for offering any new technology using spectrum across the seven frequency bands that will be offered in auction on March 1, 2021. In another positive indication reported on January 28, the Ministry of Defence and the Department of Space have agreed to vacate the 125 MHz spectrum in the 3300-3600 MHz range, paving the way for the launch of commercial 5G services. ISRO has agreed to leave the 25 Mhz spectrum in the 3300-3600 Mhz band and the Navy has agreed to use 100 Mhz in a lower frequency band, to make available the entire 300 Mhz in this band as requested by telecom operators.[9]

India aspires to join the global ecosystem of 5G that is developing in the low-band (under 1GHz), mid-band (3.3-3.5GHz) and high/millimeter wave bands (above 24GHz). As per the GSMA study of 2019, millimeter wave-based 5G alone will account for $212 billion of GDP growth in APAC by 2034. Of this, South and South East Asia will account for $45 billion of GDP growth, with the growth being largely generated by India.

Telecom service providers have, therefore, urged the DoT to ensure allocation of at least 400 MHz per telecom operator in millimeter wave bands. Internet service providers (ISP) have also urged the government to change the rules and allocate millimeter spectrum to ISPs, to enable them to provide fixed wireless access (FWA) broadband to households and enterprises.[10]

There are also conflicting demands for E (71-76GHz) and V (57-64GHz) Bands of spectrum for back haul communication along with 6 GHz spectrum for the new Wi-Fi technology. All these contentious spectrum-related issues are being deliberated by a committee set up under Cabinet Secretary Rajiv Gauba in 2020.[11]

In December 2020, the government had issued the National Telecom Security Directive which is slated to be implemented in 180 days from the date of approval.[12] The move has been perceived as a proactive step aimed at keeping

[9] https://www.bloombergquint.com/economy-finance/space-dept-defence-min-agree-to-vacate-spectrum-worth-rs-60-000-cr-for-5g-services
[10] https://telecom.economictimes.indiatimes.com/news/internet-service-providers-want-5g-spectrum-urge-india-to-allow-them-to-participate-in-auctions/80213926
[11] https://telecom.economictimes.indiatimes.com/news/defence-space-departments-likely-to-vacate-spectrum-for-commercial-5g-services/80446274
[12] ET Telecom January 22, 2021,

Chinese gear makers Huawei and ZTE out of India's 5G deployments. The committee, headed by the National Cyber Security Coordinator (NCSC), needs to consider the legal ramifications of the directive, including accountability in case of a security breach on trusted equipment used in a telecom network.

Launch of quantum computing applications lab

Quantum computing is an emerging field that harnesses the laws of quantum mechanics to build powerful tools to process information. The Ministry of Electronics and Information Technology, in a press release on January 19, announced the launch of the World's first quantum computing applications lab on a Amazon Web Services (AWS) platform to support the national government's mission to drive innovation. AWS will provide hosting with technical and programmatic support for the Lab. This MeitY initiative will provide scientific, academic, and developer communities access to a quantum computing development environment aligned with the government's science and technology priorities.[13]

Private sector in Space

Amazon Web Services (AWS) and OneWeb are among the 22 firms that have shown interest in opening up space business in India and put forward their proposals to the Indian National Space Promotion and Authorisation Centre (IN-SPACe) in December 2020.

Bharti Group-backed UK-based OneWeb said on January 14 that it has received additional funding from SoftBank Group Corp. and Hughes Network Systems LLC, bringing its total funding to $1.4 billion with the aim of launching a first-generation satellite fleet, totalling 648 satellites, by the end of 2022. OneWeb has proposed to provide services in India.[14]

Capability Building with Artificial Intelligence

India is a member of the Global Partnership on AI that was launched in 2018, to guide "the responsible development and use of AI". The G20 Digital Ministers adopted a declaration to promote a human-centered approach to artificial intelligence (AI) and support for the G20 AI Principles. In October 2020, India organised the Responsible AI for Social Empowerment (RAISE) Summit, evoking a large response.

[13] https://pib.gov.in/PressReleasePage.aspx?PRID=1690085
[14] https://telecom.economictimes.indiatimes.com/news/bharti-backed-oneweb-gets-fresh-funding-from-softbank-hughes/80283898

Taking a step towards 'Atmanirbhar Bharat' the Indian Army, on January 11, awarded a landmark $20 million (nearly ₹140 crore) contract to Indian drone maker ideaForge for an undisclosed number of indigenous tactical drones. Each 6.5 kg 'SWITCH' is a fixed wing VTOL (vertical take-off and landing) UAV that can be deployed at high altitude and in harsh environments for day and night surveillance in intelligence, surveillance and reconnaissance (ISR) missions with range up to 15 km from altitudes of 4,000 meters. The drones will be provided on priority to Indian Army troops and special forces units deployed across the friction points of eastern Ladakh.[15]

[15] https://www.livefistdefence.com/2021/01/indian-army-hands-landmark-20-million-deal-to-indian-drone-pioneer-ideaforge.html

International Developments

Activities in Global Cyber Space

On January 6, 2021 the world woke up to the shock of the US Capitol building siege, aided by digital platforms that demonstrated how digital technology enabled both the insurrection and subsequent legal accountability. Besides technology, the incident brought out the powers of dominant digital corporations to exercise control over political communication. The platforms' role as gatekeepers of content and inconsistent follow up actions, including banning of the US President, are seen as threats to democratic and free speech norms.

The reform of Section 230 to impose accountability without complete elimination of the legal liability shield has been under discussion in the US. Also, regulatory controls are being attempted to rein in these behemoth companies.

The actions by incumbent monopolies to deplatform Parler, a free-speech competitor to Twitter, to stop further violence after the riot at the Capitol on January 6, was considered controversial and an attempt to penalise new rivals.

The SolarWinds hack reported last month has compromised at least half a dozen US cabinet departments and an unknown number of private companies. In a joint statement on January 5, four US agencies in charge of intelligence and cybersecurity attributed the attack to an advanced, government hacking group "likely Russian in origin" which is responsible for most or all of the cyber compromises of both government and non-governmental networks. While the statement did not identify the agencies compromised, those affected reportedly include the departments of State, Treasury, Commerce and Energy. Further investigation results and response of the new US administration will be keenly watched.

Geopolitical contest over Semiconductor Technology

Semiconductor chips have become the latest faultline of geopolitical contestation. Taiwan, and the world's largest contract chip manufacturer, Taiwan Semiconductor Manufacturing Company Limited (TSMC), which is the producer of chips for Apple Inc. smartphones, artificial intelligence, automobile and high-performance computing, is at the centre of this contest. This is one of the technologies that makes China dependent on the global supply chain. China imports more than $300 billion of semiconductors. While TSMC holds the dominant position in the supply of smaller, more powerful

chips that require less energy, other countries in this complex supply chain include the US for chip design and software tools, the Netherlands for fabrication machines and Japan as the key supplier of equipment, chemicals and wafers.

The dominant position of TSMC can be gauged from the fact that it posted a net profit of $5.1 billion in 2020 and is likely to raise capital expenditures of between $25 billion and $28 billion, boosting capex by at least 47% in 2021. There is a comprehensive ecosystem in Taiwan around TSMC, including ASE Technology Holding which is the world's top chip assembler and MediaTek as the largest smartphone chipset vendor.

Because of increased demand of semiconductor-based devices due to Covid-19, there has been an acute shortage in the automobile industry that has become increasingly driven by chips. The US, the EU and Japanese automakers are lobbying their governments for help, with Taiwan and TSMC being asked to step in. These countries are also investing to boost chip production. The US is establishing a $12 billion chip fabrication plant in Arizona. South Korea's Samsung Electronics Co. is set to follow, with a $10 billion facility in Austin, Texas. In 2020, Japan had earmarked ¥110 billion ($1 billion) for R&D investment and another ¥90 billion for 2021 that likely includes the plan for setting up a TSMC facility in Japan.

Semiconductor chips have thus become a strategic asset and TSMC's chip-making skills have handed Taiwan political and economic leverage amid the technology standoff between the U.S. and China, which is unlikely to ease under the new US administration.

China's push for self-reliance in Semiconductors

China finds itself suddenly decoupled from this global supply chain. Its top chipmaker, Semiconductor Manufacturing International Corp (SMIC), as well as Huawei, is on the US Entity List. Therefore, China has articulated the goal of "technology independence" in the 14th five-year plan with an investment of $1.4 trillion through 2025. Last year, after the US imposed restrictions, Huawei had invested in several chip making sectors dominated by companies from the U.S., Japan, South Korea and Taiwan, such as chip design tools, semiconductor materials, compound semiconductors and chip production and testing equipment.[16]

[16] https://asia.nikkei.com/Spotlight/Huawei-crackdown/Huawei-ramps-up-chip-investment-in-fight-for-survival

On January 22, Chinese budget phone maker Honor, earlier a part of Huawei, reportedly signed partnerships with major chip suppliers such as Intel and Qualcomm and struck deals with technology firms including AMD, MediaTek, Micron Technology, Microsoft, Samsung, SK Hynix, and Sony.[17] The ongoing technology war with the US may push China to nurture several semiconductor champions, to become self-sufficient in the long run.[18]

Experts also believe that Beijing could resort to stealing chip IP from Taiwanese companies. On January 27, it was reported that the Taiwanese cybersecurity firm TeamT5 has observed a steady increase in attacks on the Taiwanese semiconductor industry since the tightening of U.S. export controls on China. Alarmed by a ransomware attack on TSMC, the Taiwanese government announced grants of $500 million to help the industry become more aware of cybersecurity issues.[19] The greater worry is that TSMC's chip factories could become victims of collateral damage if China were to make good on threats to invade Taiwan.

Space War between China and the US

Space is becoming the next great power contest between the US and China. Chinese antisatellite weapons and powerful laser beams threaten American satellite fleets, thus denying the US a technological edge. While the development of swarms of tiny satellites as well as fleets of reusable rockets have made antisatellite targeting difficult, Chinese cyberattacks can effectively cut off communication with these satellites that track enemy movements, relay communications among troops and provide information for the precise targeting of smart weapons.

Gen Lloyd J. Austin, the US Secretary of Defence, in his Senate Armed Forces Committee testimony for confirmation on January 19, said that he would update the Defense Department's National Defense Strategy and called for 'orbital resilience', 'laser like focus' and partnerships with commercial space entities for innovations to maintain and sharpen the U.S. "competitive edge" against China's increasingly powerful military. He also called for new American investment in "space-based platforms".[20]

[17] Reuters January 22, 2021, 10:39 IST
[18] https://www.caixinglobal.com/2020-11-20/chinas-stumbling-sprint-to-semiconductor-self-sufficiency-101630701.html
[19] https://teamt5.org/en/posts/stormmedia-bloomberg-the-world-is-dangerously-dependent-on-taiwan-for-semiconductors/
[20] https://www-nytimes-com.cdn.ampproject.org/c/s/www.nytimes.com/2021/01/24/us/politics/space-war-takeaways-us-china.amp.html

Chinese Regulatory control on technology giants

China has released new draft antimonopoly rules for its online platforms on January 24, adding to efforts in the US and the EU to curb the power of digital companies. Earlier in November, China unveiled its first draft guidelines overseeing competitive behavior by digital giants which included regulatory requirements on shareholders, management, sources and uses of funding, risk management and corporate governance. In January, China heightened scrutiny of electronic-payment companies, warning that nonbank payment firms, if found to be dominating the market, could face antitrust investigations.[21]

On January 29, it was reported that the Ant Group, whose $37-bn IPO was suspended last November, is planning to turn itself into a financial holding company, overseen by China's central bank, to conform to the above-mentioned regulations. The company has submitted an outline restructuring plan, to be effective in mid-February, for approval by the Chinese Financial Stability and Development Committee, chaired by Vice Premier Liu He. The future of Ant's nonfinancial businesses such as blockchain-technology development, digital-lifestyle services and artificial-intelligence technology is not known yet.[22]

[21] https://www.wsj.com/articles/china-is-joining-the-global-push-to-rein-in-tech-giants-11611484200

[22] https://www.livemint.com/companies/news/jack-ma-s-ant-plans-major-revamp-in-response-to-chinese-pressure-11611857764183.html

International Cooperation

India-Japan Cooperation in ICT

On January 15, India and Japan signed an MoU to enhance cooperation in the field of Information and Communications Technologies, to cooperate across 5G, telecom security, submarine optical fiber cable and smart cities, spectrum management, high altitude platform for broadband in unconnected areas, disaster management and public safety. Govt organisations such as C-DOT and ITI Limited along with industry partners from Japan will also form part of this cooperation.[23]

[23] https://pib.gov.in/PressReleasePage.aspx?PRID=1688812

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

www.delhipolicygroup.org