



Delhi Policy Group

Advancing India's Rise as a Leading Power



DPG CYBER REVIEW

FEBRUARY 2021



Volume II, Issue 2 | February 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. II, Issue 2

February 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

© 2021 by the Delhi Policy Group

Delhi Policy Group

Core 5A, 1st Floor,

India Habitat Centre,

Lodhi Road, New Delhi- 110003.

www.delhipolicygroup.org

DPG Cyber Review
Vol. II, Issue 2
February 2021

Contents

Abstract	i
National Developments	1
Challenges posed by Social Media in Indian Cyberspace	1
Regulatory Measures for Social Media	1
Measures to address digital fraud	3
Liberalisation of geospatial data.....	3
India's readiness for the roll out of 5G	4
Draft National Strategy on Blockchain.....	4
Indian plans for sovereign digital currency.....	5
Budgetary Support.....	5
International Developments	6
Attacks on Global Cyber Space.....	6
Myanmar Curbs on Social Media.....	6
Australia's Faceoff with social media on news content.....	7
China's anti-monopoly regulation.....	7
Geopolitical contest over Technology standards.....	8
China's trial of digital currency	8
International Cooperation	10
US-Taiwan Cooperation in ICT	10

Abstract

The start of 2021 has seen a spurt in unilateral actions by social media platforms in determining their privacy and content rules, in disregard of national laws. In the Indian context, the reluctance of Twitter to block posts responsible for inciting violence on January 26 and the adoption of new privacy rules by WhatsApp have been particularly significant.

To regulate these platforms, the Indian government has notified 'The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021', which mandates requirements of due diligence, adherence to the Indian Constitution and to the rule of law.

India saw the second largest (after Japan) number of cyberattacks among Asia Pacific in 2020, most of them directed at the finance and insurance sectors. In response, multi-pronged efforts are being made by national regulators to address digital fraud.

The Indian government has eased regulations governing the acquisition and application of geospatial data. Maps/Geospatial Data finer than one meter accuracy can only be created and/or owned by Indian Entities and must be stored and processed in India for better data security. Simultaneously, the Department of Space has signed a memorandum of understanding with the digital mapping company MapmyIndia to offer a fully indigenous mapping portal and geospatial services.

On the international front, the US authorities are continuing investigations of the SolarWinds hack. The Biden NSC has outlined measures for addressing security gaps, and technology companies are also discussing measures to deal effectively with cyber-attacks.

Australia passed a 'News Media and Digital Platforms Mandatory Bargaining Code Bill 2020' on February 25, generating a global tussle between the social media and news media companies regarding payment for news content hosted on digital platforms.

Technology standards are gaining urgency as rules are being decided for emerging technologies dependent on 5G networks, driverless vehicles, smart cities and the Internet of Things. China has been dominating in this field and is planning to soon unveil China Standards 2035. A group of 12 technodemocracies (T-12), including India, is being proposed to collaborate in setting standards to curb China's dominance.

National Developments

Challenges posed by Social Media in Indian Cyberspace

The tendency of social media platforms to disregard national laws and impose their own rules regarding privacy or content has posed a major challenge for the Indian government. Some of these platforms were used by national and global activists to propagate misinformation or incitement of violence, most recently at the Red Fort on January 26, when protests against farm laws were reportedly hijacked by malign elements.¹

When asked by the Indian government to remove nearly 1,200 accounts linked to entities provoking violence and disturbing public order, Twitter initially showed reluctance on grounds of protecting freedom of expression.² The government highlighted that while freedom of speech and expression is guaranteed as a Fundamental Right under Article 19 (1) of the Indian Constitution, this freedom is not absolute and is subject to reasonable restrictions as mentioned in Article 19 (2). Twitter relented after it was warned of strict action for failure to crack down on inflammatory content, in compliance with the country's laws, irrespective of Twitter's own rules and guidelines.³

Another social media platform, WhatsApp, announced on February 18 that its privacy policy update will go into effect on May 15,⁴ ignoring concerns of users for breach of privacy of Indian data, a matter pending before the Indian Supreme Court. WhatsApp, however, provided assurances that it will abide by Indian laws.⁵

Regulatory Measures for Social Media

To regulate these platforms, on February 25 the Indian government notified 'The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021'. These rules make a distinction between social media intermediaries and significant social media intermediaries, based on the number of users. An element of due diligence by significant social media

¹ <https://ciso.economictimes.indiatimes.com/news/is-the-toolkit-epicentre-in-india-or-abroad-police-track-digital-footprint/81075871>

² <https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=1696945>

³ https://www.business-standard.com/article/economy-policy/lot-of-concerns-about-behaviour-of-big-tech-firms-piyush-goyal-121021701408_1.html

⁴ <https://www.financialexpress.com/industry/technology/whatsapp-to-move-ahead-with-controversial-take-it-or-leave-it-privacy-policy-update-despite-indias-strong-stand-against-it/2197881/>

⁵ ET Government February 22, 2021

intermediaries has been prescribed, failing which the safe harbour provisions under Section 79 of the Information Technology (IT) Act would cease to apply to these platforms.

Social media platforms have been mandated to take down flagged posts within 36 hours and provide information, including verification of identity, to lawfully authorised agencies within 72 hours. The rule stipulates that encrypted messaging apps, including WhatsApp, Signal and Telegram, would identify the first originator of the information on its computer resource, as may be required by a court order or an order passed under Section 69 of the IT Act. The measures also include “grievance redressal mechanisms” for users to counter false news and violent material. Rules about digital media and over-the-top (OTT) platforms focus more on in house and self-regulation wherein a robust grievance redressal mechanism has been provided.⁶

Quest for Indigenous Apps

While these regulatory measures are timely, it should be acknowledged that India has little to show in the social networking app space, unlike China and the US. Efforts are being made by the government and Indian entrepreneurs to build indigenously developed products, but these need to be scaled up.

India's multilingual micro blogging platform ‘Koo’ has gained popularity after the current standoff with Twitter. ‘Koo’ has, however, found itself in the midst of several controversies, including a data leak row and Chinese investment. According to a French hacker, the ‘Koo’ app is leaking personal data of its users. However, these shortcomings have been dismissed as ‘teething trouble’ by Koo founders.⁷

Amidst an outcry against WhatsApp’s new privacy policy, an indigenous instant messaging app ‘Arattai’ has been launched, which derives its name from the Tamil word for ‘chit-chat’ and claims to be a safe and secure messaging platform with stringent data privacy clauses. ‘Arattai’ is yet to attract sizeable adopters from among those looking to move away from WhatsApp, Signal or Telegram. In the public sector, the National Informatics Centre has launched a government instant messaging systems or GIMS, called ‘Sandes’.

⁶ <https://pib.gov.in/PressReleasePage.aspx?PRID=1700749>

⁷ <https://ciso.economictimes.indiatimes.com/news/were-building-in-public-join-us-koo-blasts-privacy-critics/80876009>

Open initially only to government officers, it has now been released for the common public.⁸

Measures to address digital fraud

The rising popularity of non-banking financial companies (NBFCs) along with e-commerce has expanded the scope of digital fraud. Over 290,000 cyber security incidents related to digital banking were reported in 2020. According to an IBM report released on February 24, India had the second highest number of cyber-attacks after Japan in the Asia-Pacific region in 2020. Finance and insurance were the top sectors of industry in India to face these attacks. Multi-pronged efforts are being made by Indian regulators to address the menace.

On February 15, the Telecom Ministry announced the setting up of a 'Digital Intelligence Unit' (DIU) for speedy investigation and resolution of financial fraud and unsolicited messages, in coordination with various law enforcement agencies, financial institutions and telecom service providers. The central government has also launched a National Cyber Crime Reporting Portal, 'www.cybercrime.gov.in', to enable citizens to report complaints pertaining to all types of cybercrimes.⁹

On February 15, the markets regulator SEBI announced the setting up of a Cyber Security Fusion Centre for monitoring cyber security-related events in the securities markets, for faster detection and response.¹⁰ Further, the Reserve Bank of India (RBI) published detailed guidelines on February 19 to strengthen India's digital payments architecture and improve security, control and compliance among banks, gateways, wallets and other non-banking entities.¹¹

Liberalisation of geospatial data

Announcing a new mapping policy on February 15, the Indian government eased regulations governing the acquisition and application of geospatial data, allowing local startups and companies to create next-generation geospatial maps and use them to build new businesses. Maps/Geospatial Data of spatial accuracy/value finer than one meter can only be created and/or owned by Indian Entities and must be stored and processed in India for better data

⁸ <https://indianexpress.com/article/explained/explained-sandesh-the-governments-new-instant-messaging-platform-7189759/>

⁹ <https://www.thehindu.com/news/national/govt-to-set-up-digital-intelligence-unit-to-deal-with-telecom-frauds/article33848268>

¹⁰ <https://ciso.economictimes.indiatimes.com/news/sebi-mulls-cybersecurity-fusion-centre-for-securities-market/80917338>

¹¹ <https://ciso.economictimes.indiatimes.com/news/rbi-sets-rules-for-digital-payments-in-india/81121268>

security. The decision will unlock opportunities for applications of geographic information system (GIS) in the fields of agriculture, mining, water, urban utilities, public safety and infrastructure, which rely heavily on geospatial infrastructure to drive innovation and build scalable solutions.¹²

In tandem with the liberalisation, on February 11 the Department of Space signed a memorandum of understanding with the digital mapping company MapmyIndia to offer a fully indigenous mapping portal and geospatial services. The joint platform will combine the power of MapmyIndia's digital maps and technologies with ISRO's catalogue of satellite imagery and earth observation data.¹³

India's readiness for the roll out of 5G

The Parliamentary Panel on IT, in its report released on February 8, flagged India's lack of preparedness for rolling out the latest 5G telecom services due to various factors including inadequate availability of spectrum, high spectrum prices, poor development of use cases, low status of fiberisation of towers, non-uniform right of way (ROW) issues, deficient backhaul capacity, etc. The Committee remarked that 5G trials are an essential prerequisite for building the 5G ecosystem.¹⁴

Heeding the advice of the panel, the Department of Telecommunications (DoT) indicated that 5G trials are to start in next 2-3 months. DoT has received 16 applications for 5G field trials using imported as well as indigenous technology. It is setting up India-specific 5G use case labs in areas like education, health care, agriculture, public safety, and fintech. A multi-institute 'Indigenous 5G Test bed' is expected to be ready by October 2021. The test bed is likely to enhance national capability in telecom technology, develop indigenous Intellectual Property (IP) and give a fillip to Indian telecom manufacturers.¹⁵

Draft National Strategy on Blockchain

There have been two recent developments in the field of Blockchain technology. In January 2021, the Ministry of Electronics and Information Technology (MEITY) released a 'Draft National Strategy on Blockchain' for

¹² <https://telecom.economictimes.indiatimes.com/news/ashutosh-sharma-the-bureaucrat-behind-new-mapping-policy-opens-up-on-indias-rs-1-lakh-crore-game-changing-move/81133836>

¹³ PTI February 12, 2021

¹⁴ <https://www.indiatoday.in/technology/features/story/5g-in-india-are-we-there-yet-1769386-2021-02-15>

¹⁵ <https://economictimes.indiatimes.com/industry/telecom/telecom-news/expected-by-oct-5g-test-bed-to-boost-telecom-technology/articleshow/81245539.cms>

public comments by February 16. The strategy aims to create a 'National Level Blockchain Framework' which will be a multi-layered blockchain infrastructure that will host sector specific blockchains. The strategy has identified legal and regulatory challenges to adoption of blockchain, including privacy related challenges.¹⁶

Indian plans for sovereign digital currency

While the government is promoting the use of blockchain across various use-cases, India lacks a regulatory framework on cryptocurrency. During the month, the government announced that it would introduce a 'Cryptocurrency and Regulation of Official Digital Currency Bill, 2021', which will ban "private" crypto-currencies while at the same time providing the RBI with the requisite legal powers to develop a central bank-backed digital currency (CBDC).¹⁷ The initiative will boost the use of block chain technology and fintech innovation in the country.

Budgetary Support

India's 2021-22 budget recognises the role played by technology, infrastructure, innovation and start-ups in boosting the economy. During her Union Budget 2021-22 speech on February 1, the Finance Minister earmarked Rs.1,500 crore (US\$204.5 million) to provide financial incentives to upscale digital payments. On February 24, the Union Cabinet approved the Production Linked Incentive (PLI) Scheme for IT hardware products, including Laptops, Tablets, All-in-One Personal Computers (PCs) and Servers. Incentives worth Rs.7,350 crore (US\$1 billion) will be provided over four years for the manufacturing of these products in India. This comes after the success of the scheme for manufacture of mobiles and telecom equipment, announced last year.¹⁸

¹⁶ <https://www.meity.gov.in/content/draft-national-strategy-blockchain>

¹⁷ Lok Sabha Bulletin Part II for the Budget Session 2021 of Parliament.

¹⁸ <https://www.pib.gov.in/PressReleaseDetailm.aspx?PRID=1700425>

International Developments

Attacks on Global Cyber Space

US authorities are yet to unravel the full scope of the SolarWinds hack that gave hackers complete access to files and emails from at least nine US government agencies and about 100 private companies. To address security gaps exposed by the hack, Anne Neuberger, the newly appointed Deputy National Security Adviser for cyber and emerging technology, identified a range of remedial measures on February 17 which will be part of an upcoming executive order due to be signed by President Joe Biden.¹⁹ Separately, on February 23, the US Senate Intelligence Committee held its first public hearing on the SolarWinds breach. At the hearing, the chief executives from technology companies discussed and debated the reliability of cloud computing vis a vis more traditional on-premise data-storage systems, or a mix of both in a construct called hybrid-cloud, to provide robust security of critical data.²⁰

The US President, making his first major international address on February 19 to the Munich Security Conference, called for shaping the rules that will govern the advance of technology and the norms of behavior in cyberspace, artificial intelligence and biotechnology. He called for collective security efforts to protect computer networks in the United States and across Europe and the world.²¹

Myanmar Curbs on Social Media

Days after seizing power, the military rulers in Myanmar, on February 5, banned Facebook, Twitter and other social media platforms.²² The military was also reported to be drafting a Cyber Law, that has been opposed by leading internet companies, civil society and business bodies.²³ Facebook, used by about half of Myanmar's 53 million people, has emerged as a key platform for opposition to the coup. On February 24, Facebook barred Myanmar's military from its

¹⁹ <https://www.whitehouse.gov/briefing-room/press-briefings/2021/02/17/press-briefing-by-press-secretary-jen-psaki-and-deputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-february-17-2021/>

²⁰ WSJ Technology analysis, Feb. 27, 2021

²¹ <https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/02/19/remarks-by-president-biden-at-the-2021-virtual-munich-security-conference/>

²² <https://telecom.economictimes.indiatimes.com/news/myanmar-military-rulers-order-block-on-twitter-instagram-until-further-notice/80717617>

²³ Reuters February 11, 2021

platforms and barred military-owned businesses from advertising on Facebook.²⁴

Australia's Faceoff with social media on news content

Australia's News Media and Digital Platforms Mandatory Bargaining Code Bill 2020', which was passed on February 25, had generated interest globally. The legislation mandates big tech and social media giants like Facebook and Google to pay media companies for the news content that is published on their platforms.²⁵ After an initial protest, Google entered into deals with large media companies, while Facebook initially suspended several Australian accounts. The legislation was finally passed with modifications, after an agreement between Facebook and the Australian regulatory authorities was reached to permit social media platforms to strike commercial deals with Australian media organizations to pay for content. The legislation requires tech companies and news publishers to submit to binding arbitration, after due mediation process, if a deal cannot be reached on payment for content.²⁶ Facebook restored the suspended accounts subsequently.

Following this tussle, political leaders across globe have increased scrutiny on tech giants while news outlets have ramped up pressure on the platforms to cut deals. The European Union had passed copyright law in 2019 that created new copyright control for press outlets over the use of their publications on the internet by tech companies, which has been implemented by France. During the legislation process, Australia had reached out to India, Canada, Germany, France and Finland to garner support.²⁷ In a major development in India, the Indian Newspaper Society (INS), on February 25, asked Google to share 85 per cent of advertising revenues earned on news content, citing its recent agreement to compensate and pay the publishers in France, the European Union and in Australia.²⁸

China's anti-monopoly regulation

China, on its part, has also tightened regulatory measures on tech giants. On February 7, the State Administration for Market Regulation (SAMR), China's market regulator, released new anti-monopoly guidelines that bar companies from a range of behaviour, including forcing merchants to choose between the

²⁴ <https://www.nytimes.com/2021/02/24/technology/facebook-myanmar-ban.html>

²⁵ <https://telecom.economictimes.indiatimes.com/news/australia-proposes-partnership-with-india-others-against-global-tech-giants/81123799>

²⁶ REUTERS By Mike Cherney Updated Feb. 23, 2021

²⁷ REUTERS By Jeff Horwitz and Sarah E. Needleman Updated Feb.23, 2021 8:07 pm ET

²⁸ <https://economictimes.indiatimes.com/industry/media/entertainment/media/ins-wants-google-india-to-compensate-newspapers-share-ad-revenues/articleshow/81210765.cms>

country's top internet players, price fixing, restricting technologies and using data and algorithms to manipulate the market.²⁹

Separately, an agreement was reached between Jack Ma's Ant Group and the regulators, that would place its major businesses under a financial holding company overseen by government watchdogs. Hangzhou-based Alibaba said in a statement on February 2 that it has established a special task force with leaders from relevant business units to conduct internal reviews, as part of its efforts to cooperate with the antitrust investigation under the State Administration of Market Regulation (SAMR).³⁰

Geopolitical contest over Technology standards

Technology standards are gaining urgency as rules are being decided for emerging technologies dependent on 5G networks, driverless vehicles, smart cities and the Internet of Things. New fields, including facial recognition, touch on privacy and public safety, with consequences for human rights and national security. The countries and companies that set advanced technology standards have a valuable first-mover advantage.

With the aim to dominate technical standards underpinning information and communications technologies and other emerging fields, Beijing plans to unveil China Standards 2035. China's regional governments provide annual stipends of up to one million yuan, about \$155,000, for companies leading development of international standards at ISO and other bodies. Huawei, which holds the most 5G patents (followed by US chip maker Qualcomm), also leads in standards proposals at meetings of the Third Generation Partnership Project (3GPP), the global organisation that sets 5G standards.³¹

To counter China's hold over emerging technologies, particularly for AI, facial recognition or 5G that have global implications, there is a move to form a T-12 Group of Techno-Democracies, including India.

China's trial of digital currency

Amidst the US-China trade war, China is making efforts to reduce its reliance on the US dollar by increasing the global use of the yuan. It is also making a concerted efforts to popularise its digital currency. The digital yuan, known officially as the Digital Currency Electronic Payment (DCEP), is part of China's

²⁹ Reuters February 07, 2021

³⁰ <https://sg.news.yahoo.com/alibaba-promises-cooperation-antitrust-probe-121004720.html>

³¹Annual report of the US-China Economic and Security Review Commission, released in December 2020

plan to move towards a cashless society. Beijing and Suzhou carried out the latest trials of the digital currency ahead of the Lunar New Year. A joint venture between SWIFT and both the Digital Currency Research Institute and the China National Clearing Centre within the People's Bank of China (PBOC), is reportedly working for the development of the digital yuan that could help promote its international use.³²

³² <https://www.scmp.com/economy/china-economy/article/3120955/china-digital-currency-beijing-suzhou-confirm-latest-trials-e?>



International Cooperation

US-Taiwan Cooperation in ICT

On February 5, Taiwan and the US, held their first economic dialogue since the inauguration of US. President Joe Biden. The talks took place after the Taiwanese government received requests from the US, Germany and Japan for help in alleviating an unprecedented auto chip shortage that has forced major car manufacturers to cut back production. Taiwan has asked the Taiwan Semiconductor Manufacturing Company (TSMC), to fast-track production of car-related chips. This chip shortage has also highlighted the strategic importance of Taiwan, with its flagship tech industry and complete hardware supply chain.³³

³³ https://asia.nikkei.com/Economy/US-and-Taiwanese-companies-vow-to-collaborate-on-chip-supply-chain?campaign_id



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

www.delhipolicygroup.org