Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

NOVEMBER 2022

Volume III, Issue 11 | November 2022

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. III, Issue 11
November 2022

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

This monthly publication is intended to cover major developments in cyber and digital technology domains and serve as a point of reference for national stakeholders committed to making cyber space a secure, trusted and vibrant tool for India's development and economic prosperity. It also aims to foster global cooperation to establish the rule of law in the cyber space. 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. 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. III, Issue 11
November 2022

Contents

Abstract

Medical and health systems world-wide are regularly targeted by ransomware attacks and India has been a major victim for long. During the month, AIIMS, India's premier health institution, has been subjected to ransomware attack. Its digital hospital services could be restored only after 6 days of efforts by security agencies. While initiatives have been taken at the policy level to meet such challenges, capability building for hosting resilient networks and practical global cooperation among law enforcing agencies of nations are becoming increasingly important.

The Indian government remains focussed on the faster rollout of 5G services through telecom reforms and relaxation of regulatory norms, while Indian telecom operators and device makers are working together for better compatibilities. Concerns over the likely interference of 5G services in the C-Band frequency range (4-8 GHZ) with aircraft altimeters are also being addressed by regulatory authorities.

The Indian government released the draft Digital Personal Data Protection Bill, 2022 (DPDP) for public consultation and comments by December 17. The draft Indian Telecommunication Bill, 2022 that seeks to do away with the Indian Telegraph Act, 1885, the Indian Wireless Telegraphy Act, 1933, and the Telegraph Wires (Unlawful Possession) Act, 1950, remains under review after public consultations.

As militaries world-wide develop cyber warfare capabilities, the International Committee of the Red Cross (ICRC) has called on the international community to develop a 'digital emblem' under international humanitarian law, like the recognisable red-on-white emblems used in physical conflict zones, to protect ICRC's medical and humanitarian infrastructure from digital harm.

The US authorities announced new restrictions on the import or sale of communications and surveillance equipment from China because this poses an "unacceptable risk" to the country's national security. The US also has urged its allies to join its measures imposing chip technology export curbs against China.

Japan formally joined NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE) as a contributing participant. India and Australia convened their fifth bilateral Cyber Policy Dialogue, which saw discussions on a range of issues, including cyber threat assessment, next-generation telecommunications capacity building, and cooperation in the Indo-Pacific region.

National Developments

Premier Indian Health Institution attacked by Ransomware

On November 23, a ransomware attack on the All-India Institute of Medical Science (AIIMS) affected its digital hospital services, forcing it to work on manual mode.[1] On November 30, AIIMS authorities announced restoration of the hospital's e-data, with assistance from security agencies.However, its online hospital services are yet to be operational due to the volume of the data and the requirement to sanitise large number of servers/computers.[2] The attack comes within a month after AIIMS announced that it would go paperless from January 1, 2023, and be fully digitised by April 2023.

Medical and health systems world-wide are regularly targeted by ransomware attacks. India has taken diplomatic initiatives for international cooperation against ransomware attacks. On September 23, the Quadrilateral Security Dialogue (QUAD) foreign ministers deliberated on the approach to tackle ransomware and other cyber threats[3]. Likewise, on November 1, the US-led Counter Ransomware Initiative (CRI) of 36 countries and the EU deliberated on cooperation around technical aspects and law enforcement to build resilience against ransomware attacks.[4] At the Meeting, the Indian National Cyber Security Coordinator underscored the need "to support, analyse, and collaborate on counter ransomware activities".[5]

The incident underlines the need to enhance capability building for hosting resilient networks across all critical sectors, proactive cyber threat intelligence and global tactical cooperation among security agencies to establish the rule of law in cyberspace.

5G roll out in India: an update

On November 25, the Indian Telegraphy Right of Way (RoW) Rules, 2016 were amended, indicating continued focus on faster 5G rollout in the country[6]. The

[1] https://www.moneycontrol.com/news/india/aiims-cyberattack-exposes-the-vulnerability-of-indian-healthcare-9599771.html
[2] AIIMS restores data, online services to take time to resume, CIO News, ET CIO (indiatimes.com)
[3] https://www.state.gov/quad-foreign-ministers-statement-on-ransomware/
[4] FACT SHEET: The Second International Counter Ransomware Initiative Summit | The White House
[5] Grouping steps up efforts against ransomware, India a key partner | Latest News Delhi - Hindustan Times
[6] The Right of Way (RoW) in the telecommunications sector is referred to as the legal framework for setting up telecom towers, laying optical fibre cables (OFC), improving coordination among companies, and settling disputes.

amended rules stipulate harmonious and reasonable RoW charges across all states, with a single window clearance for installation of 5G small cells and optical fibre cable on street furniture.[7] Over 13 states/UTs in India have already implemented the central RoW policy, bringing down the average time for approval.[8]

In September, the Indian aviation regulator flagged concerns over the likely interference between the aircraft altimeters[9] and the 5G telecom services that operate in the C-Band frequency range (4-8 GHZ), potentially posing a challenge to safe airline operations. On November 28, it was revealed that the aviation and telecom departments are working on a plan, that includes telecom companies setting up 5G networks infrastructure away from the flight path around airports, carrying low power signals in such areas and a plan to upgrade the altimeter of all aircraft operating in the country by August 2023.[10]

Telecom and mobile industries are also active for early roll out of 5G. Airtel has commenced 5G services in eight cities, in non-standalone mode (NSA) utilising the existing 4G infrastructure, while Reliance Jio is conducting beta trials of its 5G services in five cities, in the standalone (SA) mode. Smartphone manufacturers are upgrading software to make the devices compatible to receive 5G signals. 5G enabled devices of Apple will support 5G in 200 cities by March 2023 and enable country-wide coverage by end 2023.[11]

India at the forefront of responsible and trustworthy AI

On November 22, the 4th session of the Global Partnership on Artificial Intelligence (GPAI) in Tokyo, elected India as the incoming Chair for 2023, while Japan was elected as Lead Chair for 2023, to promote a resilient society through AI deployment and empowerment of citizens. GPAI is an international initiative to support responsible and human-centric development and use of AI. It is a 29-member body created in 2020 after the G7 group decided on a multilateral think tank to consider the impacts of AI.[12]

[7] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1854472
[8] 5G in India: RoW Rules Amended by Telecom Minister (ampproject.org)
[9] A radio altimeter is an instrument that provides direct-height-above-terrain information to various aircraft systems.
[10] Safe flying: New SOP soon on 5G airwave infra around airports | Business News,The Indian Express
[11] Jio and Airtel add 3,500 5G sites per week in ramp up - The Economic Times (indiatimes.com)
[12] The 29 members of the GPAI are Argentina, Australia, Belgium, Brazil, Canada, Czech Republic, Denmark, France, Germany, India, Ireland, Israel, Italy, Japan, Mexico, the Netherlands, New Zealand, Poland, the Republic of Korea, Senegal, Serbia, Singapore,

The ministerial meeting Reaffirmed commitment to AI Principles developed by the Organisation for Economic Co-operation and Development (OECD), which are based on human-centred values, based on trustworthy, responsible, and sustainable use of artificial intelligence. The OECD's AI Governance principles complements GPAI's project-based approach, supporting collaboration with the Multistakeholder Expert Group (MEG).[13]

India, as the incoming Chair of the GPAI, has called for the development of global standards to ensure that artificial intelligence does not harm humanity and to evolve a common framework of rules and guidelines about data governance. AI is expected to add $967 Bn to Indian economy by 2035 and $450–500 billion to India's GDP by 2025.[14]

Earlier on November 21, the University of Oxford released a report, titled 'Stepping into the new digital era: how and why digital natives will shape the world', as part of the Network Readiness Index 2022. The report placed India on top of the global AI talent concentration. The NRI-2022 report ranks a total of 131 economies, based on their performances in four different pillars: Technology, People, Governance, and Impact.[15]

India launches CBDC pilot project in wholesale sector

To meet the challenges of private and volatile crypto currencies, over 100 countries are exploring their own Central Bank Digital Currency (CBDC). CBDC could become a tool for reducing time and cost for cross-border transactions.

On November 1, the Indian Reserve Bank (RBI) has launched its first e-Rupee pilot in the low volume, high-value wholesale (e₹-W) segment. The pilot in the retail segment (e₹-R) is planned next, in closed user groups comprising customers and merchants. The pilot involves nine public and private sector banks, along with other private stakeholders (technology enablers, merchants, users) to foster a broader sense of ownership, and increase the probability of successful adoption.[16]

Slovenia, Spain, Sweden, Türkiye, the United Kingdom, the United States, and the European Union.

[13] GPAI Ministers' Declaration 2022 - GPAI
[14] https://pib.gov.in/PressReleasePage.aspx?PRID=1877739
[15] India: India secures 1st rank in 'AI talent concentration' on Network Readiness Index 2022, overall 61st among 131 countries, Government News, ET Government (indiatimes.com)
[16] Rbi: RBI to commence first e-Rupee pilot in wholesale segment on Nov 1, nine banks to participate, BFSI News, ET BFSI (indiatimes.com)

Draft Digital Data Protection Bill unveiled for public consultation

On November 18, the Indian government released the Digital Personal Data Protection Bill, 2022 (DPDP), for public consultation and comments by December 17. The reworked version of the data protection Bill eases cross-border data flows and increases penalties for breaches. The Bill gives exemption to security agencies in the interest of sovereignty and integrity of India, security of the state, friendly relations with foreign states, maintenance of public order or preventing incitement to any cognisable offence. Certain businesses are also exempted based on number of users and the volume of personal data processed.

The new Bill would relax data localisation requirements and allow data flows to trusted geographies. The conditions for selecting such regions would be based on their data security landscape and ease of access to data of Indians from there.[17] The draft also proposes amendments to the Right to Information Act 2005, relating to disclosure of personal information.[18]

Draft Telecom Bill, 2022 under review after public consultations

The draft Indian Telecommunication Bill, 2022 seeks to bring in a new uniform law by doing away with the Indian Telegraph Act, 1885, the Indian Wireless Telegraphy Act, 1933, and the Telegraph Wires (Unlawful Possession) Act, 1950. Public comments on the draft were sought till November 20. The Bill seeks to bring in clarity around spectrum allocation, reduce litigation, relax right-of-way guidelines, protect consumers, and preserve competition. The Bill seeks to expand the definition of telecom services to include over the-top (OTT) communications players including WhatsApp, Signal and Telegram, under telecommunication services. The provision remains contentious. The Telecom Regulatory Authority of India (TRAI) experts are studying these issues with a view to create a level playing field among various service provisioning mechanisms, "to iron out the inconsistencies created by technological disruptions".[19]

[17] The Digital Personal Data Protection Bill, 2022.pdf (meity.gov.in)
[18] Digital Personal Data Protection Bill Proposes To Amend RTI Act To Completely Bar Disclosure Of Personal Information (livelaw.in)
[19] Trai: Trai working on light-touch norms for OTT platforms: Chairman PD Vaghela, Telecom News, ET Telecom (indiatimes.com)

International Developments

WhatsApp data breach affecting users in 84 countries

On November 28, it was reported that WhatsApp database of 487 million WhatsApp users, from 84 countries around the world including India, have been stolen and put on sale on a "well-known hacking community forum". Over 32 million of the leaked records are from users in the US, followed by the UK, Egypt, Italy, Saudi Arabia, Türkiye, and Russia. From India, more than 6 million WhatsApp users are reportedly at risk. The information on WhatsApp was obtained by harvesting information at scale, also known as scraping. The stolen data could be sold or used for marketing or phishing.[20]

Meta Fined $276 Million in Europe for Data-Scraping Leak

On November 28, Ireland's Data Protection Commission, fined Meta headquartered in Dublin, about $276 million, for not safeguarding personal phone numbers and other profile information of more than 530 million Facebook users in 2021, from data scrapers. Malicious actors had misused a Facebook tool called "Contact Importer" to upload a large volume of phone numbers, to scrape the data.

The EU has been aggressive of late in applying the General Data Protection Regulation (GDPR), to fine large technology companies. Last year, the regulator had fined Meta and its subsidiaries, including WhatsApp and Instagram, more than $900 million in a privacy case. In July, the bloc has enacted two new laws- the Digital Markets Act and the Digital Services Act, aimed at big technology companies to limit anticompetitive conduct, and to regulate content-moderation systems.[21]

INTERPOL coordinates crack down on online cyber crimes

It was revealed on November 26, that an INTERPOL-coordinated operation brought together 22 jurisdictions around the world, including Japan, India, China, Singapore, and the Republic of Korea, to cooperate against online fraud, underlining the global threat of cyber-enabled financial crime. The operation codenamed HAECHI-II, saw police arrest more than 1,000 individuals and intercept nearly $27 million of illicit funds. In addition, 2,350 bank accounts linked to the illicit proceeds were blocked. The operation tested a new global stop-payment mechanism – the Anti-Money Laundering Rapid Response

[20] https://cybernews.com/news/whatsapp-data-leak/
[21] Facebook Parent Meta Fined $276 Million in Europe for Data-Scraping Leak - WSJ

Protocol (ARRP) – which proved critical to successfully intercept illicit funds cases and understand new criminal modus operandi.[22]

Such operations highlight the importance of global cooperation and coordination among national law enforcement authorities to effectively tackle exponential increase in cybercrimes including ransomware.

El Salvador to Set Up 'National Bitcoin Office'

On November 28, El Salvador has announced the setting up of the 'National Bitcoin Office' (ONBTC), that will operate as a dedicated administrative unit to monitor local crypto projects in the region. Last year, El Salvador President declared Bitcoin as legal tender across the country. The objective of the ONBTC will be to design, diagnose, plan, program, coordinate, follow up, measure, analyse, and evaluate projects related to Bitcoin for the economic development of the country. All public institutions related to Bitcoin will have to collaborate with the ONBTC to devise profitable and safe products and services needed for crypto expansion. It will also collaborate with other countries when required.[23]

Red Cross seeks Digital Emblem for Cyberspace Protection

As militaries develop cyber capabilities, warfare and attacks are increasingly moving into cyberspace. In physical conflict zones, recognisable red-on-white emblems on persons or objects had protected humanitarian infrastructures from harm under the international humanitarian law, but there is no such protection from cyber-attacks on digital infrastructures.

On November 3, the International Committee of the Red Cross (ICRC) presented a report titled "Digitalising the Red Cross, Red Crescent and Red Crystal emblems", that called on countries to support the idea of a digital emblem that would help protect humanitarian infrastructure against erroneous targeting.[24] The report makes an initial assessment of the main benefits, risks and challenges associated with a 'digital emblem', and proposes different technical solutions and possible ways forward.

In January, the ICRC itself fell victim to a massive cyber-attack in which hackers seized the data of more than half a million extremely vulnerable people, including some fleeing conflict, detainees, and unaccompanied

[22] More than 1,000 arrests and USD 27 million intercepted in massive financial crime crackdown (interpol.int)
[23] El Salvador to Set Up 'National Bitcoin Office': All You Need to Know | Technology News (gadgets360.com)
[24] Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems | ICRC

migrants. The hackers accessed data from at least 60 national Red Cross and Red Crescent societies around the world.

For the "digital emblem" to become a reality, nations would have to agree to make it a part of international humanitarian law alongside the existing humanitarian insignia. The emblem should be able to identify the computer systems of protected facilities much as a red cross or crescent on a hospital roof does in the physical world. Discounting the apprehension that such an emblem could present "soft targets" to malicious actors, the ICRC Director General urged the international community to develop "concrete ways to protect medical and humanitarian services from digital harm during armed conflict."[25]

US and its allies to join China chip export curbs

It was reported by Nikkei Asia on November 2, that the U.S. is urging its allies including Japan and Netherlands to follow its lead on restricting exports of advanced semiconductors and related technology to China. Companies in both countries are strong in semiconductor manufacturing equipment, which so far has not been subject to U.S. regulations.

The 'Advanced Semiconductor Materials Lithography' (ASML) of the Netherlands is one of the world's largest developer, manufacturer and supplier of semiconductors manufacturing equipment using Lithographic technology with net sale of 18.6 billion Euros. Japan's Tokyo Electron hold 90% share of the global market for equipment that forms circuits by applying specialized chemicals on semiconductor wafers. The US semiconductor industry want these companies to share the burden of the export curbs to China.[26]

The US has also signed an agreement with Japan in May, to cooperate on creating a resilient semiconductor supply chain. A joint research hub with the U.S. is also being set up. On November 11, Japan unveiled a company named Rapidus, with eight companies, including Toyota Motor, NTT, Sony Group and SoftBank, to make chips with 2-nanometer technology by 2027. Taiwan Semiconductor Manufacturing Co. and South Korea's Samsung Electronics have established mass production technology at the 3-nm level and plan to mass-produce at the 2-nm level in 2025.[27] The US has blocked export/sale of these advanced technologies from China.

[25] Red Cross Eyes Digital Emblem for Cyberspace Protection | SecurityWeek.Com
[26] U.S. calls out Japan and Netherlands over China chip curbs - Nikkei Asia
[27] Japan's new chipmaker seeks to break free from 'lost decade' - Nikkei Asia

US Bans Chinese Telecom and Surveillance firms Over Security Risk

On November 25, US authorities announced new restrictions on the import or sale of communications equipment from China's Huawei Technologies and ZTE because they pose an "unacceptable risk" to the country's national security. Earlier, Huawei was banned from supplying to US government systems, with fears that its equipment could be compromised by Chinese intelligence. The US FCC also prohibited selling or importing surveillance equipment manufactured by China's Dahua Technology, video surveillance firm Hangzhou Hikvision Digital Technology and telecoms firm Hytera Communications Ltd.

The current move is the latest in a series of actions to limit the access of Chinese telecoms firms in United States networks amid a long-running standoff between the world's two biggest economies.[28]

Xi Jinping urges global technology cooperation

On November 9, Chinese President Xi Jinping called for global cooperation in the technology sector at the opening of the World Internet Conference (WIC), that promotes China's model of cyberspace governance. The event saw the debut of the Communist Party's new propaganda chief, Li Shulei and virtual attendance by global tech executives, including the CEOs of IBM, Intel and CISCO.

The debut speech of Li Shulei expounded China's contributions in "building a community with a shared future in cyberspace" while referring to the white paper released by the Cyberspace Administration of China (CAC) – the country's internet watchdog. The key theme of the summit was industrial digitalisation, away from consumer technology, with a strengthened emphasis on the integration of the country's digital and "real" economy. It was indicated that Beijing will stick to the concept of "development and regulation in parallel" for internet platform operators.[29]

[28] https://www.securityweek.com/many-potential-backdoors-found-huawei-equipment-study

[29] Xi Jinping urges global tech cooperation as IBM, Intel, Cisco CEOs attend China's internet conference | South China Morning Post (scmp.com)

International Cooperation

Japan joins NATO Cooperative Cyber Defence Centre of Excellence

On November 4, Japan formally joined NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE) as a contributing participant. Tokyo had first proposed joining the CCDCOE in 2018. The CCDCOE was founded in 2008 to serve as NATO's cyber defense research and training hub, focusing on research, training, and exercises. CCDCOE experts authored the Tallinn Manual 2.0, considered by many as the most comprehensive guide on how International Law applies to cyber operations. Even before the formal induction, Japan participated in the yearly CCDCOE cyber war game, Locked Shields, in 2021 and 2022. It is the second Asian country to join the CCDCOE after South Korea joined in May 2022.[30]

Security experts attributed Japan's move to reflect an intersection of two increasingly important considerations in Japanese security thinking; the criticality of diverse international partnerships in a difficult geopolitical environment, and the need to integrate cybersecurity with the national security policy.[31] However, Chinese experts have criticised the move saying that its real purpose is to acquire a strong group offensive capability through the military alliance.[32]

Fifth Bilateral India- Australia Cyber Policy Dialogue

On November 17, India and Australia convened their fifth Bilateral Cyber Policy Dialogue, that provides a bilateral platform to discuss a range of issues of mutual interest, including strategic priorities, cyber threat assessment, capacity building for next generation telecommunications, cooperation in the Indo-Pacific region, and the latest developments in cyber at the United Nations.

Australia and India agreed to explore opportunities for further collaboration with the private sector and academia, including through the Australia-India Cyber and Critical Technology Partnership. Australia and India will jointly conduct a Cyber Bootcamp, as well as Cyber and Technology Policy Exchanges, in collaboration with Indo-Pacific partners.[33]

***

[30] https://www.theregister.com/2022/11/07/japan_joins_nato_cyber_defence/
[31] https://therecord.media/japan-formally-joins-nato-cyber-cooperation-center/
[32] https://www.scmp.com/news/china/diplomacy/article/3198898/china-casts-wary-eye-japan-signs-nato-cybersecurity-platform
[33] MEA | Statements : Press Releases

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

www.delhipolicygroup.org