Delhi Policy Group
Advancing India's Rise as a Leading Power

DPG Cyber Review

Volume 1, Issue 6

JULY 2020

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. 1, Issue 6
July 2020

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 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 for Cyber Security and Digital Technologies at abhi.ghosh@dpg.org.in

Cover Photographs:

Prime Minister Narendra Modi interacting with Google CEO Sundar Pichai on July 13, 2020.
Source: https://twitter.com/narendramodi

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

DPG Cyber Review, Vol. 1, Issue 6
July 2020

Contents

Abstract

The month of July, 2020 witnessed a number of national and international developments related to Cyberspace with geopolitical implications.

Cyber-attacks on Indian Banking Services and Information Infrastructure from China continued unabated, but reportedly without much success.

The Indian Government undertook scrutiny of Chinese Apps, Chinese digital equipment deployed on Critical Infrastructure, and Chinese investors in Indian start-ups because of concerns regarding China's military-civil fusion policy.

India's telecommunications companies requested the government to expedite the 5G Spectrum auction for trial and roll out of networks, leveraging the global ecosystem around the 26 GHz band, besides other bands of the Frequency Spectrum.

Reliance Jio indicated it has developed its own end-to-end 5G technology which is awaiting trial and commercialisation, a development that may herald indigenous alternatives to reliance on Chinese equipment.

India's commitment to emerging technologies, including Artificial Intelligence for inclusive growth and development, was the highlight of the Prime Minister's online conversation with Google CEO Sundar Pichai on July 13, 2020.

As countries around the world tighten data privacy and security within their borders, India is moving to draft and reinforce policies governing the use of both personal and non-personal data.

Google announced plans to invest $10 billion in India over the next 5-7 years, to "accelerate digitisation" in India, of which an investment of Rs. 33,737 crores ($4.5 billion) will go to its capability building initiatives with Reliance Jio.

On the international front, US-China, US-Russia, UK-Russia and Israel-Iran face offs in cyberspace continued. The governments of the US, UK and Canada named Russia-based hackers for attacks on virus vaccine research infrastructure. US Security Agencies issued a cybersecurity alert to operators of critical infrastructure in view of heightened tension with adversaries.

The US Senate voted to incentivise domestic semiconductor manufacturers, while the US Department of Energy (DOE) prepared a strategy for the development of a national quantum internet.

The US and Russia held inconclusive Space Talks on July 27, 2020 amidst allegations by the US that Russia had conducted the trial of an anti-satellite weapon.

The UK banned Huawei from Britain's 5G network and ordered telecom companies to remove all existing Huawei gear from their networks by 2027, while France urged telecom operators to avoid sourcing from Huawei.

National Developments

Cyber Threat Scenario

Two Chinese firms traced as sources of mass hacking attacks

Two Chinese hackers – Gothic Panda and Stone Panda – have been traced as the alleged orchestrators of a majority of hacking attacks on Indian entities, as reported on July 24, 2020. They are said to have targeted websites of banking and information management services for 'Internet Protocol Hijack' and 'Distributed Denial of Service' (DoS) attacks. These non-state actors are allegedly known to act at the behest of Chinese Agencies.

Cyber attackers put out details of some stolen NHAI files

Days after a Maze ransomware attack on NHAI's mail server, details of some of the stolen files surfaced on the internet, as reported on July 4, 2020. The attackers have leaked two data sets relating to a former NHAI chairman and a former senior official. Experts from CERT-IN, the national nodal agency for responding to computer security incidents, have visited the NHAI office and are investigating the matter.

Chinese companies in India under scanner over 'links' with PLA

It was reported on July 19, 2020 that after India's move to ban 59 Chinese Apps in June, 2020 and restrictions on Huawei and ZTE's participation in 5G business, a number of Chinese companies in India, as well as investors in start-ups, are under scrutiny for their alleged links to the Chinese government's military-civil fusion policy.

India's Information Technology Ministry has given these companies three weeks to respond to a questionnaire, including whether they censored content, worked on behalf of foreign governments, lobbied influencers or whether they acted at the behest of any foreign government to edit, promote or demote any content.[1]

Power Sector industry reaches out to alternative supply chain

Cyber threats to Critical Information Infrastructure like the Power Sector, affecting national security and economy, have been a longstanding national concern.

[1] Reuters | July 15, 2020, 08:02 IST

Indian Electrical & Electronics Manufacturers' Association President R. K. Chugh said on July 20, 2020 that power distribution and transmission gear companies have begun mass cancellations of orders on Chinese companies and are reaching out for MoUs with reliable and friendly countries including Japan, Taiwan, Korea, Germany, Russia, the Czech Republic and Poland.

The Indian government is also finalising a proposal to set up an Electronics Commission to reduce import dependence on China and work towards removing roadblocks in manufacturing of electronics in order to steer growth of the sector.[2]

Coordinated social engineering attack hits Twitter

Twitter acknowledged that on July 16, 2020 hackers had taken control of its internal system and tools, after hijacking several Twitter accounts of high-profile people, tech billionaires and companies and offering to send $2,000 for every $1,000 sent to a bitcoin address.

The Indian Computer Emergency Response Team (CERT-IN) asked Twitter about Indian users affected by the hacking. CERT-IN also sought information on Indian users, remedial measures taken by Twitter to prevent attacks of this nature in the future, the vulnerability exploited by the attackers and modus operandi of the attack.[3]

Digital Technologies

PM Narendra Modi and Google CEO Sundar Pichai discuss Emerging Digital technologies

On July 13, 2020, Prime Minister Narendra Modi held a wide ranging conversation with Google CEO Sundar Pichai, focusing particularly on leveraging the power of technology to transform the lives of India’s farmers, youth and entrepreneurs. They also discussed the emerging work culture stemming from the coronavirus pandemic. Pichai reportedly mentioned the launch of an AI research lab in Bengaluru and highlighted the benefits of Google's flood forecasting efforts.

[2] https://telecom.economictimes.indiatimes.com/news/electronics-commission-in-the-works-to-reduce-its-import-dependence-on-china/77232277

[3] https://inc42.com/buzz/indias-nodal-agency-for-cybersecurity-issues-notice-to-twitter-over-recent-hack/

Communication Technologies

Telcos urge DoT to release 26 GHz band of Spectrum for 5G use

Lt Gen SP Kochhar (Retd), Director General of the Cellular Operators Association of India (COAI), told ET on July 21, 2020, that India's telecommunications companies have asked the government to include the mmWave 26 GHz band in the 5G spectrum auction to help roll out cost-efficient networks and price their services more affordably. They fear India could lose out on leveraging the global devices ecosystem rapidly developing around the 26 GHz band. DoT has so far earmarked Frequency spectrum in the 3.3-3.6 GHz band for 5G.

5G Technology

Reliance Jio develops 5G solutions for commercial deployment

Reliance Jio announced on July 15, 2020 that it has designed and developed its own complete 5G solutions, which will be ready for trial and for field deployment by 2021. The trials will be launched as soon as the 5G spectrum is allocated.

Having developed end-to-end 5G technology, Jio will be able to offer a wide array of services like security and surveillance using drones, industrial IoT, and applications in the agriculture sector.

Reliance Jio has asked the DoT to allocate 800 megahertz in the 26 GHz and 24 GHz bands, and 100 MHz in the 3.5 GHz band, for field trials using its own 5G technology in Mumbai and New Delhi.

US cyber diplomat tells global telcos to follow Reliance Jio model

Robert L. Strayer, the US Deputy Assistant Secretary for Cyber and International Communications and Information Policy, told IANS on July 22, 2020 that the United States is urging telecom operators around the world to follow the Reliance Jio template of developing homegrown 5G solutions, while criticising Huawei and the consequences of "untrusted" Chinese components in 5G infrastructure.

Artificial Intelligence

"Implications of AI on the Indian Economy"

A study by Google, Nasscom and ICRIER titled "Implications of AI on the Indian Economy" has indicated that a unit increase in AI intensity by Indian firms can result in a 2.5 per cent increase in the country's GDP in the immediate term.

Launching the report at a webinar on July 24, 2020 the CEO of Niti Aayog, Amitabh Kant, stated that "By integrating new technologies like AI and ML into various sectors, India can radically leapfrog and catch up with advanced economies".

Responsible AI for Youth

With the objective to empower India's youth to become AI ready and help reduce the skills gap, the National e-Governance Division of the Ministry of Electronics and Information Technology and Intel India have designed a **National Programme for Government Schools: Responsible AI for Youth**. The aim of this initiative is to provide students a platform to acquire appropriate new age skill-sets and prepare them for a digital future.

Quantum Technology

Experts planning for quantum-resistant cryptography

Advances on large quantum computers carry major consequences for cybersecurity. In the future, even robust cryptographic algorithms are likely to be substantially weakened by quantum computing.

Researchers in India have been working on a public-key cryptography algorithm that can counter code-breaking efforts by quantum computers. The US National Institute of Standards and Technology (NIST) is also evaluating new standards for "post-quantum cryptography", to be ready by 2024.[4]

[4] ETCIO July 03, 2020

Strategy/Regulation/Policy

I-T dept to share financial data with 10 investigative and Intelligence Agencies under NATGRID

The Income Tax Department will share PAN and bank account details of any entity with 10 investigative and intelligence agencies, including the CBI and the NIA, under the integrated counter-terrorism platform, National Intelligence Grid (NATGRID), to help track suspects and prevent terrorist attacks with real-time data and access to classified information like immigration, banking, individual taxpayers, air and train travel.

Parliament IT panel discusses data security and privacy

The Parliamentary Standing Committee on Information Technology, headed by Shashi Tharoor, met on July 14, 2020 to discuss the ban on 59 Chinese Apps last month, and sought details from government officials on data security and privacy of Indian citizens. The Panel asked whether some crucial data could already have landed in the hands of the Chinese in the last few years. The threat of sharing personal data through the Covid-19 contact tracing App, Arogya Setu, also came up during the meeting.

Personal Data Protection Bill 2019

The personal data protection Bill 2019 is currently undergoing review by a Joint Parliamentary Committee (JPC) of the Parliament. The JPC, headed by Meenakshi Lekhi, was convened on July 27, 2020. Representatives from the Ministry of Home Affairs, Ministry of Electronics and Information Technology, National Investigation Agency (NIA), the Narcotics Control Board (NCB) and the Census Commissioner deposed before the members. The Committee is learnt to have focused on exemptions for government agencies under the Data Protection Bill. The JPC deliberations are to continue.[5]

Report on Draft Non-Personal Data Framework

Non-Personal Data is the fuel for the growth of Artificial Intelligence in the country. The Report on a Non-Personal Data Framework was released by MEITY's Committee of Experts on July 12, 2020 for public comments by August 13, 2020. The Committee, headed by Kris Gopalakrishnan, has recommended that separate legislation be formulated to govern non-personal data and a new regulatory body be set up. The rules proposed in the report would govern

[5] https://www.medianama.com/2020/07/223-jpc-pdp-bill-july-27-meeting/

collection, analysis, sharing, distribution of gains, as well as the destruction of data. Non-personal data refers to information that does not include any details such as name, age or address that could be used to identify an individual.

Capability Building

Airtel and Reliance Jio launch Video Conferencing Platforms

Bharti Airtel and Verizon on July 14, 2020 joined hands in a strategic alliance to bring a secure, world-class video conferencing solution to India, as an alternative to other video conferencing apps such as Zoom, Microsoft Teams and Google Meet.

As part of the deal, Airtel will offer its secure enterprise-grade video conferencing solutions under the brand name Airtel BlueJeans to enterprise customers.

Similarly, Reliance Industries has launched unlimited free conferencing app JioMeet as a competitor to Zoom. The JioMeet video conferencing app is available across Android, iOS, Windows, macOS and web since July 23, 2020.[6]

Google to invest $ 10 Billion in India Digitisation Fund

On July 13, 2020 Google announced plans to invest $10 billion in India over the next 5-7 years, to "accelerate digitisation". The fund will focus on enabling affordable access to the Internet in own language; leveraging technology and artificial intelligence for digital literacy; outbreak predictions; and support for rural economies.

As a follow up, Reliance Jio announced that Google is investing Rs. 33,737 crores ($4.5 billion) in its Jio Platforms initiative, with a 7.7 percent stake in the company. Google thus joins Facebook, Intel and Qualcomm in the growing list of investors in Jio Platforms.[7]

[6] https://economictimes.indiatimes.com/tech/internet/jiomeet-takes-on-zoom-can-support-up-to-100-participants/printarticle/76763423.cms

[7] https://www.androidauthority.com/google-jio-investment-1138029/

International Developments

Cyber Threat scenario

U.S. Indicts Two Chinese Nationals for Hacking

The United States Department of Justice on July 21, 2020 accused two Chinese hackers of stealing hundreds of millions of dollars of trade secrets from companies across the world and more recently targeting firms developing a vaccine for the coronavirus. The indictment alleges that besides acting for their own profit, the duo also engaged in the stealing of information which was of interest for the Chinese Ministry of State Security (MSS).

Russian Hackers Blamed for Attacks on Coronavirus Vaccine-Related Targets

On July 16, 2020 the Russian hacking group APT 29, also known as Cozy Bear, was blamed by the U.S., U.K. and Canadian governments for ongoing cyber espionage against organisations involved in the development of coronavirus vaccines and other health-care-related work.

The trio's conclusions were based on assessments by Britain's National Cyber Security Centre (NCSC) and its counterparts in the US and Canada. On July 19, 2020 Russia's Ambassador to Britain rejected these allegations.[8]

Cyber intrusion into Britain’s Critical National Infrastructure

Britain’s Intelligence and Security Committee (ISC) warned on July 21, 2020 that since 2014, Russia has "undertaken cyber pre-positioning activity on other nations’ Critical National Infrastructure (CNI)” - including intrusions in the UK. The report observed that Russian GRU actors have orchestrated phishing attempts against government departments and that there is a nexus between business, corruption and state power in Russia.

Iran-Israel Cyber-attacks on Critical Infrastructures escalate

On July 02, 2020, Iran reported a major blast at its nuclear plant in Natanz. Security agencies have not yet revealed the full details, but signs point towards

[8] https://ciso.economictimes.indiatimes.com/news/russian-ambassador-rejects-virus-vaccine-hacking-claims/77058870

a cyber-attack. Iran's Civil Defence Head warned that Iran will retaliate against any country that carries out cyber-attacks on its nuclear sites.

Israel reported on July 17, 2020 that two cyber-attacks were carried out against Israeli water infrastructure in recent weeks; however, no damage was done to Israel's water system.[9]

US NSA, CISA tighten Critical Infrastructure Security

On July 23, 2020 the U.S. National Security Agency and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency issued a cybersecurity alert to operators of critical infrastructure, outlining "immediate actions" that should be taken during a "time of heightened tensions" to avoid being compromised by a cyberattack. The warning could be related to tensions with several adversaries of the United States, including Russia, China and Iran.

US Confirms Cyberattack on Russian Troll Farm

In an interview with the Washington Post on July 10, 2020, President Trump confirmed that a cyberattack was launched in 2018 against a Russian company, the Internet Research Agency (IRA), believed to be behind major disinformation campaigns and online influence operations for the Russian government. The goal was to prevent Russia from interfering in the 2018 midterm elections.

Digital Technologies

US Senate votes to subsidize domestic Semi conductor manufacturers

The US Senate voted mid July to subsidise domestic manufacturers of semiconductors to compensate for the restrictions imposed on them on grounds of national security. The measure was passed as an amendment to the National Defense Authorisation Act. Senator John Cornyn, who co-sponsored the amendment, noted that for America to maintain its preeminence, both from a national-security and an economic perspective, a federal incentive program through the Department of Commerce is required to encourage semiconductor manufacturing.

[9] Cyber-attacks again hit Israel's water system, shutting agricultural pumps | The Times of Israel

UK Government bid to acquire satellite technology firm under probe

A UK parliamentary panel has launched an inquiry into the UK government's successful bid to acquire satellite technology firm OneWeb along with India's Bharti Enterprises early in July. As part of the deal, the UK will invest USD 500 million worth in equity shares in London-based OneWeb, while another USD 500-million will come from Bharti Global Ltd.

U.S., Russia Hold Talks on Space Security

On July 27, 2020 the U.S. and Russia held their first space-security talks since 2013 in Vienna. The two major space powers are at odds over goals. The US seeks the establishment of a set of voluntary norms for operating in space and possibly a new communications channel to link space officials on each side. Russia on its part has advocated a formal treaty against the placement of weapons in space.

The inconclusive talks came amidst allegations from the U.S Space Command on July 23, 2020 that Russia had tested an Anti-Satellite Weapon on July 15 in order to improve its capability to attack American space-based systems. Russia has denied the allegations and claimed that it was carrying out a trial of a new "inspector satellite" that is intended to monitor Russian space assets in orbit.[10]

5G Technologies

UK bans Huawei from 5G networks

UK announced on July 14, 2020 that it will ban Huawei from Britain's 5G network, ordering telecoms companies to remove all existing Huawei gear from the 5G network by 2027 and not to purchase 5G components from Huawei after December 31, 2020. China's Ambassador in London, Liu Xiaoming, warned Britain not to treat China as a hostile country. The decision follows a technical review by the UK National Cyber Security Centre in response to US sanctions against Huawei.[11]

[10] https://www.wsj.com/articles/russia-tests-an-anti-satellite-weapon-u-s-officials-say-11595545670

[11] https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027

France urges 5G Telecom Companies to not use Huawei

French cyber security agency ANSSI said it would not be imposing a total ban on Huawei in the roll-out of France’s 5G network, but it was urging companies to avoid Huawei. France's decision over Huawei's equipment is crucial for two of the country's four telecoms operators, Bouygues Telecom and SFR, as about half of their current mobile network is made by the Chinese company.[12]

Quantum Technologies

US Unveils Blueprint for 'Virtually Unhackable' Quantum Internet

AFP reported on July 24, 2020 that the US Department of Energy (DOE) has prepared a strategy for the development of a national quantum internet, using laws of quantum mechanics to transmit information more securely than on existing networks. In February this year, scientists from DOE's Argonne National Laboratory and the University of Chicago had created a 52-mile (83-kilometer) "quantum loop" in the Chicago suburbs, establishing one of the longest land-based quantum networks. The aim is to create a parallel, more secure network based on quantum "entanglement," or the transmission of sub-atomic particles.

International Cooperation

Bilateral Cooperation

India and Israel sign Agreement to deal with cyber threats

India and Israel have signed an Agreement on July 16, 2020 to further expand collaboration in dealing with cyber threats amidst rapid digitisation due to the coronavirus pandemic. The Agreement lays down the framework for dialogue, cooperation in capacity building, mutual exchange of best practices in the field and facilitates regular exchanges.

15th India-EU Summit pushes cooperation in cyber space

European Council President Charles Michel and European Commission President Ursula von der Leyen, participated in the 15th India-EU virtual summit with Prime Minister Narendra Modi on July 15, 2020. The summit launched a number of initiatives in maritime security, trade and investment, law enforcement, energy, cyber space and artificial intelligence.

DST launches India-Russia Joint Technology Assessment and Accelerated Commercialization Programme

On July 23, 2020 Prof. Ashutosh Sharma, Secretary, Department of Science and Technology, launched the India-Russia Joint Technology Assessment and Accelerated Commercialisation Program in partnership with the Federation of Indian Chambers of Commerce and Industry (FICCI) and Foundation for Assistance to Small Innovative Enterprises (FASIE) of the Russian Federation. Over a period of two years, both countries will fund up to INR 15 Crores ($2 Million) each for projects that include, among others, IT & ICT, AI, Robotics and Drones.

Multilateral Cooperation

New Roadmap to Finalise OEWG Report by March 2021

On July 16, 2020 the Chair of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security ("OEWG"), in a letter to all UN member states, announced a new roadmap to allow the Group to successfully conclude its work despite the obstacles imposed by the COVID-19 pandemic.

The Group will now prepare its Report at the third and final substantive session in March 2021, so that it can be considered at the plenary session of the 75th session of the UN General Assembly in 2021.

Union Minister speaks of Data Sovereignty at G-20 Meet

On July 22, 2020 India participated in the G20 Digital Ministers' conference hosted by Saudi Arabia. Minister for Electronics and Information Technology, Ravi Shankar Prasad, emphasised the need to make digital platforms "responsive" and "accountable" towards sovereign concerns. He also spoke about "data privacy" and the need to build trustworthy "artificial intelligence" systems.[13]

[13] https://pib.gov.in/PressReleasePage.aspx?PRID=1640482

DPG

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

www.delhipolicygroup.org