Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

DECEMBER 2020

Volume I, Issue 11 | December 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 11
December 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 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. 1, Issue 11
December 2020

Contents

Abstract

2020 has been a year of disruptions, marked by a devastating pandemic and geopolitical rivalries over trade and technology. The advent of the coronavirus pandemic was historic, shifting human activity into the digital space but also creating massive security concerns for the global banking and financial sector, health care sector and research institutions. The data generated by the massive surge in digitisation, while promoting the growth of Artificial Intelligence and futuristic 5G communications, also became a target for manipulation, affecting national security and economy. Several nation states were reportedly involved in shaping online narratives, some to disinform, misinform and build new technological systems of social control.

Indian cyber space had seen a massive surge in cyberattacks across all sectors, not only due to the pandemic but also because of a collusive campaign of our adversaries in China and Pakistan. Numerous hospitals, Covid-19 research firms and pharma companies, including Dr. Reddy's Labs and Lupin, have fallen victim to ransomware in the last quarter of 2020. These targeted attacks and disinformation campaigns will surge in 2021, affecting industry, critical infrastructure and government machinery.

Timely policy interventions to protect data and national networks by banning of Chinese apps and scrutiny of supply chains of hardware/software deployed on critical infrastructures have helped to mitigate vulnerabilities. India is working on scaling up secured communication networks and boosting manufacturing capabilities by developing indigenous technologies. The auction of 4G spectrum is planned in early 2021. The roll-out of futuristic 5G networks, dependent on the readiness of the Indian eco system, needs to be fast tracked.

Internationally, the year 2020 witnessed ransomware attacks, data breaches, disinformation campaigns and even sophisticated nation-state sponsored attacks. Covid-19 vaccine research and distribution systems were among the targets of these attacks. The year ended with revelations of a massive supply chain linked cyber espionage attack across US government agencies and industry. This attack brought into stark focus the fallibility of even the most developed countries in cyber space, in spite of having well laid out strategies and spending billions of dollars on security organisations and counter measures. These attacks, by proxies or by nation states, pose grave risks to national security and should be deterred by collective punitive actions by likeminded countries, aided by their technology industries.

National Developments

Cyber Threat Scenario

Disruptions in Indian cyber space since mid-2020 have emanated both from the Covid-19 pandemic and the expansionist agenda of China on India's northern borders. The unprecedented digital transformation in all national activities has been accompanied by a massive surge in cyberattacks against Indian industry and citizens. India is amongst the top three countries in the world facing cyberattacks, including ransomware attacks. Nearly 80 lakh attacks were recorded in the last quarter of 2020 on the healthcare sector alone. India and Australia have logged the highest number of security incidents across the Asia-Pacific region, with more than 61 entities from the region breached by targeted ransomware attacks in 2020.[1]

Kaspersky has reported that cyber-attacks on India originated from several countries, including China and Pakistan, after the revocation of Article 370 by the Union government. On social media, bot-driven social media campaigns were run by Pakistani intelligence, aimed at fuelling anti-India sentiment, particularly in the Gulf countries, which are otherwise close allies of India.

Indian citizens, government and business entities faced around seven lakh cyber-attacks and lost ₹1.24 lakh crore last year. According to Delhi Police, sixty-two per cent of cybercrime complaints lodged in 2020 in the Indian capital were related to financial frauds. Several such attacks originated from the Chinese provinces of Guangdong and Henan, with proxy servers in Belgium and the US.[2]

Strengthening cybersecurity should thus be a major national focus in 2021. The National Cyber Security Strategy, due to be released shortly, is likely to address major concerns of national security. Further regulatory measures like the Personal Data Protection Bill should also be able to address the concerns of privacy and security of data. Indian industry and government need to step up collaboration on secure communication networks, indigenous manufacturing and research, development of digital technologies including 5G, AI, satellite communications and quantum computing, for a resilient Indian cyber space and 'Aatmanirbhar' Bharat.

[1] https://www.thehindubusinessline.com/info-tech/india-australia-report-the-highest-number-of-targeted-ransomware-incidents-in-apac-in-2020-report/article33318987.ece

[2] https://www.financialexpress.com/industry/sme/e-commerce-fraud-chinese-hackers-targeted-e-shoppers-during-flipkarts-festive-season-sale/2153666/

Secure Communication Network

On December 8, Prime Minister Shri Narendra Modi, speaking at the virtual India Mobile Congress (IMC) 2020, called for emphasis on secure and inclusive communication by bringing high speed fibre-optic connectivity to every village over the next three years. IMC-2020 aimed to drive foreign and local investments and encourage R&D in the telecom and emerging technology sectors.[3]

Prime Minister Narendra Modi addressing the India Mobile Congress 2020 virtually on December 8, 2020.
Source: PIB, GoI

In a move aimed to safeguard next-generation technology-based networks from cyber-attacks, data theft and other virtual vulnerabilities threatening national security, on December 16 the Indian Government approved a 'National Security Directive on the Telecom Sector'. The National Cyber Security Coordinator (NCSC) will be the "Designated Authority" to designate 'Trusted Products', based on approval by a committee headed by a Deputy NSA. From among the sources declared as 'Trusted Source' by the Designated Authority, those which meet the criteria of the Department of Telecom's 'Preferential Market Access Scheme' will be certified as 'Indian Trusted Sources'. Indian telecom service providers will be required to connect new devices which are

[3] https://pib.gov.in/PressReleasePage.aspx?PRID=1679041

designated trusted products.[4] The Department of Telecom will make appropriate modifications in the license conditions for the implementation of the provisions of the Directive. The policy will come into operation after 180 days from the date of approval.[5]

The new directive, which is in line with similar initiatives by the US and European nations, will maintain supply chain integrity to protect data and enhance resilience of telecom networks.

Broadband penetration

Internet penetration is essential for the growth of the nation. However, in spite of being the second largest user of the internet with more than 504 million active users, the majority of the country's population remains underserved. Against the targeted 10 million Wi-Fi hotspots by 2022 set by the National Digital Communications Policy 2018, India's current pan-India count is merely 1 lakh. Proliferation of telecom networks with adequate frequency spectrum bands, fibre optic networks for backhauls and public access to internet from remote corners of the country is essential.

The Union Cabinet, on December 9, accorded approval for the setting up of Public Wi-Fi Networks by Public Data Office Aggregators (PDOAs) to provide public Wi-Fi services through Public Data Offices (PDOs), akin to erstwhile PCOs, spread across the length and breadth of the country. There shall be no license fee for providing Broadband Internet through these public Wi-Fi networks. This secure public Wi-Fi, 'The Prime Minister Wi-Fi Access Network Interface' (PM-WANI), will provide stable and high-speed Broadband Internet (data) services.[6]

Further, on December 10, BSNL announced the launch of a satellite-based NB-IoT (Narrow Band-Internet of Things), indigenously developed by Skylotech India. With this solution, India will now have access to a network of connectivity for millions of yet unconnected machines, sensors and industrial IoT devices associated with fishermen, farmers, construction, mining and logistics enterprises. Skylo would also help provide critical data for the logistics

[4] https://telecom.economictimes.indiatimes.com/news/govt-sets-up-national-security-directive-to-allow-only-trusted-telecom-gear/79758205

[5] https://stratnewsglobal.com/govt-mandates-trusted-telecom-vendors-in-national-security-directive/

[6] https://pib.gov.in/PressReleasePage.aspx?PRID=1679344

sector to enable effective distribution of the COVID-19 vaccine in 2021 and will be a big contributor in this service to the nation.[7]

Availability of Spectrum

Recognising the importance of spectrum availability for the Telecom Sector, the Government of India, on December 16, approved a proposal for the auction of spectrum at the reserve price in seven frequency bands ranging from 700 MHz to 2500 MHz, for a validity period of 20 years. A total of 2251.25 MHz is being offered, with a total valuation of Rs.3,92,332.70 crore ($53.68 Billion). The auction will enable telecom service providers to renew licences and augment their 4G network capacity.[8]

Budgetary Support for 'Make in India'

To be secure and resilient, India has initiated measures to expand its manufacturing base across all critical segments. Offering production-linked incentives (PLIs) to encourage foreign and domestic firms to 'Make in India' is intended as a result-oriented initiative.

Riding on the success of this scheme for mobile manufacturing, the Indian Digital Communications Commission has approved guidelines for a nearly Rs.12,200 crore ($1.67 Billion) PLI scheme for telecom equipment manufacturing. The scheme will cover core transmission equipment, 4G/5G and next-generation radio access network and wireless equipment, access and customer premise equipment (CPE), Internet of Things (IoT) access devices and enterprise equipment such as switches and routers.[9]

India's aspiration to achieve $400 billion in electronics manufacturing by the year 2025 cannot be realised unless it produces basic components. While electronics manufacturing has steadily moved up the value chain, the domestic value addition is estimated to be only in the range of 15% - 20% and growth in manufacturing so far has primarily been driven by final assembly/Printed Circuit Board Assembly (PCBA) using imported components and sub-assemblies. The country is lacking a semiconductor manufacturing ecosystem as well as efficient electronic components.

[7] https://pib.gov.in/PressReleasePage.aspx?PRID=1679714

[8] https://pib.gov.in/PressReleasePage.aspx?PRID=1681044

[9] https://telecom.economictimes.indiatimes.com/news/dcc-approves-pli-scheme-for-telecom-gear-manufacturing/79603171 dec7

In a move aimed at incentivising and attracting investment for setting up of chip manufacturing in India, the Union Ministry of Electronics and Information Technology (MeitY) issued a notice on December 16 inviting Expression of Interest (EoI) for setting up/expansion of existing Semiconductor wafer/device fabrication (FAB) facilities in India (preferably with a node size of 28nm or lower, wafer size of 300 mm and capacity of 30,000 WSPM or more) or acquisition of Semiconductor FABs outside India.[10] Meanwhile, as reported on December 28, the Indian Space Research Organisation is planning to build an additional FAB at its Semiconductor Laboratory (SCL) to meet the growing demand for chipsets for rockets and satellites. The new FAB will build chips with 65 nm technology. SCL presently has a 180 nm facility for strategic purposes, while the Semiconductor Technology and Applied Research Centre (SITAR) has a 100 nm unit for applications in critical areas.[11]

[10] https://www.meity.gov.in/writereaddata/files/EoI_Semiconductor_FAB_dated-15122020.pdf

[11] https://economictimes.indiatimes.com/news/science/isro-eyeing-new-chip-unit-as-more-firms-take-to-skies/printarticle/79985212.cms

Capability Building to harness digital technologies

Quantum Technology

Secure communications are vital for defence and strategic agencies the world over, and distribution of encryption keys is an important requirement. Sharing of keys over the air or wired links requires encryption, which in turn requires encryption keys to be pre-shared. Quantum based communication offers a robust solution to sharing the keys securely.

The Defence Research & Development Organisation (DRDO) achieved a milestone on December 9, with the development of Quantum Communication using time-bin Quantum Key Distribution (QKD) technology, that underwent trials in Hyderabad between two DRDO labs, for secure communication. The technology will also serve to define standards and crypto policies that can leverage QKD system in a unified Cipher Policy Committee (CPC) framework for more secure and pragmatic key management for current and future military cryptographic systems.[12]

Space Technology

Within months of India deciding to open up the space sector, at least 22 proposals from Indian firms and institutions and four foreign companies are being formally reviewed by the Indian National Space Promotion and Authorization Center (IN-SPACe). The proposals range from approval for ground stations to setting up satellite constellations, making and launching satellites, launch vehicles and providing applications. US-based Amazon Web Services (AWS) and Bharti Group backed UK-based OneWeb are among the foreign firms that have shown interest in India's space sector. UAE's Archeron Group and Norway's Kongsberg Satellite Service (KSAT) have also sent proposals to the IN-SPACe.[13]

[12] https://indiaeducationdiary.in/quantum-communication-between-two-drdo-laboratories/

[13] https://swarajyamag.com/insta/indias-liberalisation-in-the-space-sector-becomes-big-hit-as-22-indian-and-4-global-firms-send-proposals

International Developments

Activities in Global Cyber Space

Digital transformation due to the pandemic had disrupted the global cyber space significantly. Ransomware attacks, data breaches, disinformation campaigns and even sophisticated nation-state sponsored attacks were reported during the year 2020. Cybercriminals have used the pandemic to launch scams and phishing attacks on critical infrastructure, social media, medical and research institutions, and individual users. Even Covid-19 vaccine research and distribution has attracted the attention of the cybercriminals. The Twitter cryptocurrency hack of accounts of major public figures including then US presidential candidate Joe Biden, Barack Obama, Elon Musk, Bill Gates and Jeff Bezos, by a "coordinated social engineering attack", has pointed to the vulnerability of cyberspace. Security firm McAfee noted that cybercrime incidents could cost the world around $1 trillion in 2020.

The biggest revelation in December 2020 was the supply chain attack and cyber espionage on several American companies and US government agencies. On December 13, the US government confirmed that its computer networks had been hit by a cyberattack, executed by exploiting the supply chain of Solar Winds's Orion network monitoring product. While the US government has not shared a list of impacted agencies, media reports indicate Departments of Commerce, Treasury, Energy and Defence, among others, were affected along with at least 24 technology companies including Intel, Cisco, VMware and Nvidia. The US National Security Council has activated a Unified Coordination Group to ensure continued unity of effort across the United States Government to respond to the incident.

The security company FireEye, which was breached in a related attack on December 8, attributed the attacks to a Russian state hacking campaign. FireEye disclosed that Solar Winds was targeted by two malwares, Sunburst backdoor and Supernova.

Operationally, the attack has exposed critical flaws in both supply chain security and cybersecurity defences, including 'Einstein', a multi-billion-dollar tool deployed by the US Cybersecurity and Infrastructure Security Agency (CISA) to detect malware.[14] It also raises questions about ignoring the basic cyber hygiene and best practices including sand boxing for remote updates of critical networks. On a higher plane, the attack rekindled the discussion regarding appointing separate Commanders for the US Cyber Command and

[14] Net Politics December 18, 2020

the National Security Agency. Both organisations currently are headed by Army Gen. Paul Nakasone, an arrangement known as "dual-hatting." Experts also doubts the efficacy of the Cyber Command strategy of 'defending forward' which apparently prevented interference of the US elections but was unable to detect intrusion into its homeland networks.[15] Speaking with the media on December 28, the US President-elect Joe Biden called for partnering with other democracies to close the gap in capabilities to better deter, detect, disrupt, and respond to these sorts of intrusions in the future.[16]

Co-located Headquarters of the US Cyber Command and National Security Agency
Source: VOA News

Elsewhere in the world, IBM researchers reported on December 03 that attackers have targeted organisations in at least six European and Asian countries. The targets appear to be associated with the Cold Chain Equipment Optimization Platform (CCEOP) of Gavi, the Vaccine Alliance, whose main goal is to improve access to vaccines in poor countries. Targets of the attack included the European Commission's Directorate General for Taxation and Customs Union, which could serve as an entry point to high-value organizations across the European Union, as well as companies in the IT, energy and manufacturing sectors that could provide access to valuable information related to the distribution of a coronavirus vaccine.[17] The North

[15] https://www.nytimes.com/2020/12/20/us/politics/nsa-cyber-command-russia-hack.html?referringSource=articleShare

[16] https://economictimes.indiatimes.com/news/international/world-news/joe-biden-sets-tone-for-us-china-ties-says-coalition-needed-to-confront-beijing/articleshow/80003228.cms

[17] https://www.securityweek.com/state-sponsored-hackers-likely-behind-attacks-covid-19-vaccine-cold-chain

Korea-linked threat actor known as Lazarus was reportedly linked to some of these attacks.

In a cyber attack on the aviation industry, Brazilian company Embraer, which is the third-largest airplane maker after Boeing and Airbus, has become latest victim of a ransomware attack, it was reported on December 7. Hackers uploaded data of Embraer employees, business contracts, photos of flight simulations and source code, among others, on the Dark Web.[18]

Cold War over Technology

While the trade war front was relatively quiet in 2020, ties between Washington and Beijing have grown increasingly antagonistic over digital technologies in 2020. The US continued its ban on sales to China of any hardware or software that contains US technology. The US also pushed forward its efforts to get countries to ban Huawei equipment from their 5G networks. China alleged that the US was intimidating countries as part of its new "Clean Network" initiative, primarily focussed on network security issues in the global rollout of 5G technologies.

In a bid by the US administration to curb access to sophisticated U.S. chipmaking technology,[19] China's largest manufacturer of computing chips, Semiconductor Manufacturing International Corp. (SMIC), alongside more than 60 other Chinese institutions, were added to an export blacklist on December 3, over their reported links to the Chinese military and intelligence communities as well as the Communist Party. The designation effectively prohibits SMIC from acquiring US technology to build chips with 10 nm circuits and smaller.

Restrictions on 5G Technology

Continuing with the technology clampdown on China, the US Federal Communications Commission (FCC), on December 11, ordered certain US telecommunications companies to remove Huawei equipment from their networks. The FCC has estimated that the programme will require at least $1.6 billion to reimburse eligible providers who take federal subsidies, mostly to provide services in rural areas of the US.[20]

[18] https://ciso.economictimes.indiatimes.com/news/hackers-leak-key-data-from-brazilian-airplane-maker-embraer/79607276

[19] https://www.wsj.com/articles/u-s-blacklists-chinas-top-chip-maker-escalating-tech-fight-11608274932?mod=searchresults_pos1&page=1

[20] https://www.bbc.com/news/business-55269879

Meanwhile, German Chancellor Angela Merkel's cabinet approved a bill on December 16 that does not outrightly ban Huawei in Germany, as demanded by the US. The bill requires companies involved in setting up critical infrastructure such as high-speed 5G networks to guarantee that their equipment cannot be used for sabotage, espionage or terrorism.[21]

Race over Quantum technology

Quantum technology has put China and the US on a competitive course. On December 4, Chinese scientists claimed development of the world's first light-based quantum computer, which can solve problems far faster than a classical supercomputer. Jiuzhang, the quantum computer, reportedly demonstrated "quantum computational advantage". China has also launched a 2,000-km "hack proof" quantum communication line between the national capital Beijing and its commercial centre Shanghai which cannot be wiretapped.[22]

Not to be outdone, NASA scientists reportedly achieved long distance quantum teleporting by sending qubits of photons through a 44 kilometer fiber-optic cable, which will revolutionise data storage and computing. This network was built using quantum entanglement, with off-the-shelf equipment, which would be compatible with existing internet infrastructure.[23]

Regulatory control on technology giants

Across the globe in 2020, the technology giants like the social media, e-commerce and fintech companies have faced rough weather with anti-trust regulators. In December, the European Commission issued a charge sheet that Amazon was abusing its dominance. European authorities are also investigating whether Amazon's algorithms do product placement unfairly.

In the United States, the federal government initiated antitrust cases against Google and Facebook, and a large number of US states collectively launched legal action on the two companies and others for a range of alleged infractions. The seemingly concerted onslaught from regulators and administrators appears designed to curb monopolistic powers of big technology companies.

[21] https://www.securityweek.com/german-government-backs-bill-requiring-5g-security-pledge

[22] https://telecom.economictimes.indiatimes.com/news/chinese-scientists-make-worlds-first-light-based-quantum-computer-report/79578795

[23] https://www.independent.co.uk/life-style/gadgets-and-tech/quantum-teleportation-nasa-internet-b1777105.html

Meanwhile, China too is coming down hard on its giant internet companies like Alibaba and Tencent. In November, the Chinese government had abruptly cancelled the world's biggest stock offering of Ant Financial, the non-bank finance arm of Alibaba. The IPO has now been indefinitely postponed.

In India too, there is increasing regulatory scrutiny of technology companies by the Competition Commission of India (CCI).

International Cooperation

Recognising the importance of multilateral and bilateral cooperation for stability in cyberspace, India on December 14 hosted the sixth edition of the India-EU Cyber Dialogue. Officials from and the European Union discussed various areas of cooperation in cyberspace, including coordination on relevant discussions at UN platforms, the Organization for Security and Co-operation in Europe (OSCE) and the ASEAN Regional Forum. They acknowledged the need to follow the basic values of both societies in cyber space and its governance, such as the rule of law, democratic values and fundamental freedoms. The next India-EU Cyber Dialogue will be held in Brussels.[24]

[24] https://www.republicworld.com/world-news/rest-of-the-world-news/india-eu-agree-to-strengthen-cooperation-in-cyberspace-at-6th-edition-of-cyber-dialogue.html

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

www.delhipolicygroup.org