Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

AUGUST 2022

Volume III, Issue 8 | August 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 8
August 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 8
August 2022

Contents

Abstract

The much-awaited Indian National Cyber Security Strategy is likely to conceptualise a "No First Use Policy" against state entities in Cyberspace, as part of an Assured Defence Posture (ADP) and "deterrence by retaliation". India has adopted several institutional and regulatory reforms in a "whole of nation approach" to strengthen its defensive posture. Among these measures, the National Security Directive on Telecom sector (NSDTS) has strengthened network security by stipulating that all products connected to the telecom network of India have to be procured and adopted from trusted sources.

Notwithstanding, India continues to be a major target for cyberattacks by state-sponsored Chinese criminal gangs. Multiple vulnerabilities are also reported in the software and hardware deployed by global companies in India, that can let hackers gain access to their computers, prompting CERT-In to issue advisories.

The controversial Data Protection Bill 2021, introduced in the Parliament in 2019, was officially withdrawn during the month. The Government is working on a new comprehensive framework of global standard laws, including Digital Privacy laws, that address contemporary and future challenges.

The spectrum auction for 5G that ended during the month was immediately followed up by necessary payments by telecom service providers (TSP) and the formal assignment of spectrum to respective TSPs, to speed up the rollout of 5G. Besides the auctioned airwaves, E-band airwaves (71-76/81-86 GHz) were provisionally allotted via the administrative route for backhaul needs.

TSPs have partnered with telecom gear makers and chip makers for their respective networks to develop an ecosystem that can serve the needs of India and beyond. An internal committee has been formed to work out a strategy to incorporate 37.0-42.5 GHz (Millimetre Wave Band) as international mobile telecommunications (IMT) bands, which will allow telecom companies to offer 5G fixed wireless access services. Enterprises willing to set up private networks are to be allotted spectrum directly from DoT.

The Supreme Court took on record the report of the expert technical committee it had constituted to investigate allegations whether the Israeli-built spyware Pegasus was used for unauthorised surveillance. The preliminary findings revealed no conclusive evidence that Pegasus was used on the 29 phones examined by the committee.

A Stanford Internet Observatory report revealed that as part of multiple covert campaigns, troll farms are using deceptive tactics to promote pro-Western narratives to social media users in the Middle East and Central Asia, for promoting the interests of the United States and its allies while opposing adversaries like Russia, China, and Iran.

Ukraine's nuclear operator "Energoatom" reported an "unprecedented" cyberattack on its website by a Telegram channel called 'Popular cyber army,' allegedly sponsored by Russia. The cyberattack came as tensions flared over the Zaporizhzhia nuclear power plant which is one of Ukraine's four nuclear power stations that supplied around half of its electricity needs before the "Russian Special Operation".

Cyber Security firm Trend Micro reported that a China-linked cyberespionage group "Iron Tiger" was observed using the compromised servers of a messaging app for targeting hundreds of organisations worldwide for cyberespionage purposes, mostly from Taiwan.

Chinese search engine giant Baidu has unveiled its first quantum computer named "Qianshi," with a 10-Qubit processor, that has been made available to external users. Global governments and companies, competing for technology supremacy, are reportedly likely to invest around $16.4 billion in quantum development by the end of 2027.

The US President signed the CHIPS and Science Act of 2022, amid competitive concerns with China over semiconductor manufacturing and technological capabilities. The Act represents a fundamental paradigm shift in the US government policy regarding subsidising this strategic sector, which has spurred technology companies to invest 'on shore' for semiconductor manufacturing.

India conducted a Cyber Security Exercise "Synergy" for 13 countries as part of the International Counter Ransomware Initiative (CRI)- Resilience Working Group. National Crisis Management groups of these countries participated in the exercise.

The United States and Israel announced the finalisation of a bilateral Memorandum of Understanding ('MoU') on Cybersecurity Cooperation.

National Developments

India conceptualises 'No First Use Policy' in Cyberspace

India's proposed National Cyber Security Strategy is likely to adopt the "No First Use Policy" in Cyberspace as part of an Assured Defence Posture (ADP). This was indicated by the National Cyber Security Coordinator (NCSC) in an interview on August 18. The Strategy proposes Cyber deterrence by enhancing offensive capabilities so that adversarial state entities do not attack for the fear of retaliation.

India has initiated several institutional and regulatory measures in the last decade to enhance its defensive posture. It created the National Critical Information Infrastructure Protection Centre (NCIIPC) in 2014 that conducted the first national cyber exercise, NCX India 2022, from April 18-29. Other agencies created to oversee and strengthen cybersecurity in different sectors include the Indian Cyber Crime Coordination Centre (I4C), the Defence Cyber Agency for the Armed Forces and the Cyber Diplomacy Division under the Ministry of External Affairs.[1]

To ensure network security, the National Security Directive on the Telecom Sector (NSDTS) was implemented from December 16, 2020, stipulating that all products connected to the telecom network of India have to be procured and adopted from trusted sources: trusted countries, companies, and their related supply chains. The Mandatory Testing and Certification of Telecom Equipment (MTCTE) was notified by the Government of India on September 5, 2017, while the responsibility for framing security-related requirements and security certifications lies with the Bengaluru-based National Centre for Communication Security (NCCS).[2]

On August 12, the Ministry of Home Affairs released a **"Cyber Pravah"** Newsletter of the I4C that includes cybercrime trends/patterns, platforms for reporting and addressing cybercrimes, and measures for cybercrime prevention, detection, and investigation by State/Central agencies working in the area of cyber security and cybercrime.[3]

[1] https://www.geospatialworld.net/prime/urgent-need-of-data-protection-framework-and-bill-in-india
[2] https://www.geospatialworld.net/prime/urgent-need-of-data-protection-framework-and-bill-in-india
[3] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1851346

China-backed hackers continue to target India

Notwithstanding the efforts made by a 'whole of nation' approach to secure Indian Cyberspace, India continues to be a major target for cyber-attacks by state sponsored criminal gangs. It was reported on August 22 that a Chinese government backed hacking group 'Red Alpha' has been attacking governments, NGOs, news publications, and think tanks globally including India's National Informatics Centre (NIC), to steal their login credentials. The group spoofed login pages for NIC, which manages Indian government networks and services. Parliamentarians, ministers, and other government officials have email ids associated with the NIC domain name. In April this year, hackers had targeted North India's power supply, gained access to the dispatch centers by compromising internet-facing camera devices, and used IOT devices as Command and Control (C&C) entities with the infected networks.[4] This hacking group has targeted organisations that "fall within the strategic interests of the Chinese government".[5]

On August 22, The Indian Computer Emergency Response Team (CERT-In) warned users about multiple vulnerabilities in Google Chrome for desktops that can let hackers gain access to computers and allow a remote attacker to execute arbitrary code and security restriction bypass on the targeted system. CERT-In also warned about multiple vulnerabilities in the Apple operating system software and in Cisco products, that can be exploited by a remote attacker by enticing a victim to open a specially-crafted file.[6]

Indian Government withdraws Data Protection Bill 2021

On August 3, the controversial Data Protection Bill 2021 was officially withdrawn from Parliament. This will be replaced by a comprehensive framework of global standard laws, including Digital Privacy laws for addressing contemporary and future challenges. The new legislation will catalyse the Indian Prime Minister's vision of making this decade an "India Techade" with a concerted push for 5G, semiconductors and transformation through digital services, boosting the technology sector in the country.

Privacy is a fundamental right of Indian citizens, and India requires globally tenable Cyber Laws to fulfil its ambition of becoming a trillion-dollar economy. On August 26, the Parliamentary Standing Committee on Information and

[4] Targeting of the Indian power grid | CFR Interactives
[5] China-backed hackers spying on govts, India's NIC among victims, IT Security News, ET CISO (indiatimes.com)
[6] google chrome: India's cyber agency warns about bugs in Google Chrome for desktop, IT Security News, ET CISO (indiatimes.com)

Technology chaired by Shashi Tharoor questioned top Twitter officials about former head of Twitter security Peiter Zatko's allegations about its India operations on issues of data security and privacy. The parliamentary committee is working on a comprehensive report on data privacy and security.[7]

India speeds up rolling out of 5G networks

The spectrum auction for 5G that ended on August 1 was followed up immediately by letters for spectrum assignment for 5G to respective telecom service providers (TSP) after initial payments of auction amounts, to speed up the roll out of 5G. Besides the auctioned air waves, the letter also provisionally allotted E-band airwaves (71-76/81-86 GHz) exclusively via the administrative route for backhaul needs.[8]

TSPs have already partnered with telecom gear makers like Ericsson, Nokia, Samsung and Cisco and chipmakers like Qualcomm for their respective 5G networks, in order to develop an ecosystem that can serve India and beyond. TSPs are also working on Drones, Robotics, Automotive, Industry 4.0, and Private Networks.[9] It was reported on August 25 that Nokia and Adani Data Networks are looking to establish 5G private networks across business areas focussing on ports and mining verticals.[10]

To speed up the process, the Government on its part has issued the 'Guidelines for Captive Non-Public Network (CNPN) licence' (Private Network) on June 27, 2022, aimed at establishing the legal framework for CNPNs. The guidelines also invite enterprises having net worth of more than Rs. 100 Crores ($ 12.5 million), and willing to set up private networks, to obtain spectrum directly from DoT.[11]

The Government has also stepped up its efforts in fielding indigenous equipment. On August 3, the Parliament was informed that the Government has funded the development of an indigenous 5G testbed by prominent academic and research institutions working in this area of technology. This

[7] Parliament panel grills Twitter officials over data security, privacy, CIO News, ET CIO (indiatimes.com)
[8] DoT catches up with 5G rollout deadline, issues spectrum assignment letter within hours of receiving payments, Government News, ET Government (indiatimes.com)
[9] Reliance Jio: Jio partners Ericsson, Nokia, Samsung, Cisco for 5G network; Google for ultra-affordable 5G smartphone, Telecom News, ET Telecom (indiatimes.com)
[10] 5G Spectrum: DoT initiates process to auction more 5G spectrum - The Economic Times (indiatimes.com)
[11] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1850446

testbed can be used for testing indigenous products, anywhere in the 5G chain, and for enabling technology proliferation.[12]

Further, on August 15, DoT constituted an internal committee to chalk out a strategy to incorporate the 37.0-42.5 GHz (Millimetre Wave Band) as international mobile telecommunications (IMT) bands, which will allow telecom companies to offer 5G fixed wireless access services.

While the International Telecommunication Union's World Radio communication Conference held in 2019 had adopted the 37.0-43.5 GHz as an additional band for IMT services, India has been lagging in notifying these bands as IMT. Besides mobile and satellite communications, this band can also be utilised for private networks.

TSPs are expected to roll out 5G in Metro cities by October 2022 and in other cities by December 2023.[13]

Huawei may scale down R&D in India amid Government scrutiny

It was reported on August 25 that the Chinese telecom gear maker Huawei is considering scaling down its research and development (R&D) operations in India which could affect its Indian employees. This comes amidst heightened scrutiny by the government from the perspective of national security, as well as income tax raids, audits, and the issuance of a lookout circular (LOC) against the chief executive of Huawei Telecommunication India. Several GOI ministries, including the Home Ministry, Education Ministry, and others have informally placed restrictions on any collaboration with the company. Huawei has shifted some of its critical development projects back to China.[14]

Updates on Pegasus enquiry

On August 25, the Supreme Court took on Record the report of the expert technical committee headed by former SC Justice RV Raveendran that it had constituted to investigate allegations whether the Israeli-built spyware Pegasus was used illegally to infect the phones of opposition politicians, judges, journalists, activists and others in India. The court had also asked the

[12] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1847831
[13] Jio 5G rollout will happen in 4 cities by Diwali: Check the full list and when your city will get 5G - Technology News (indiatoday.in)
[14] Huawei: Huawei may scale down R&D in India amid govt scrutiny, affecting most of 3,500 jobs: Report, Telecom News, ET Telecom (indiatimes.com)

committee to make recommendations on a legal and policy framework on cyber security to ensure that the right to privacy of citizens was protected.[15]

The final report was in three parts — digital images of phones examined for spyware infection, report of the technical committee, and the report of Justice Raveendran.

The preliminary findings revealed by the Apex Court found no conclusive evidence that Pegasus was used on the 29 phones it examined, though it did find unspecified malware in five of them. The Bench while releasing the Report, observed that the Government of India did not cooperate with the committee. Pegasus-maker NSO Group has consistently maintained that its spyware was for use strictly by government agencies in combating terrorism and organised crime.[16]

[15] SC wants to know who used Pegasus; independent probe ordered - The Economic Times (indiatimes.com)
[16] No evidence, Govt didn't cooperate: SC panel on Pegasus | India News, The Indian Express

International Developments

US influence campaign on Ukraine under scrutiny

On August 24, the Stanford Internet Observatory (SIO) Cyber Policy Centre released a report "Unheard Voice: Evaluating five years of pro-Western covert influence operations" that evaluated five years of pro-Western campaigns. The report revealed that as part of multiple covert campaigns, troll farms were using deceptive tactics to promote pro-Western narratives to social media users in the Middle East and Central Asia in order to promote the interests of the United States and its allies while opposing countries including Russia, China, and Iran.

Between March 2012 and February 2022, these accounts posted approximately 300,000 tweets, under two different sets of activity: the overt US government messaging campaign called the Trans-Regional Web Initiative, and a series of covert campaigns of unclear origin. Twitter said the countries of origin appeared to be the United States and the United Kingdom.[17]

In July and August 2022, Twitter removed two overlapping sets of such accounts for violating their policies regarding "platform manipulation and spam," while Meta removed some of these assets on its platforms for engaging in "coordinated inauthentic behaviour."[18]

Ukraine nuclear operator reports cyberattack on its website

On August 16, Ukraine's nuclear operator "Energoatom" reported an "unprecedented" cyberattack on its website, the most powerful cyberattack since the start of the Russian "Special Operation" against Ukraine. A Telegram channel called 'Popular cyber army', allegedly affiliated to Russian state agencies, called on its followers to attack the Ukrainian nuclear operator's website. The group used more than 7 million internet bots to attack the website for three hours. The assault, however, did not have a considerable impact on the functioning of the Energoatom website. The cyberattack came as tensions flared over the Zaporizhzhia power plant in the south of the country, which Russian forces had occupied in March. Zaporizhzhia is one of Ukraine's four nuclear power stations that supplied around half of its electricity supply before the Russian "Special Operation." Ukraine had faced the world's worst nuclear

[17] Twitter, Meta Remove Accounts Linked to US Influence Operations: Report | SecurityWeek.Com
[18] FSI | Cyber | Internet Observatory - Unheard Voice (stanford.edu)

accident in 1986, when the Chernobyl power station's reactor number four had exploded.[19]

Russia linked cyber groups also targeting organisations in Ukraine

It was reported on August 15 that a Russia-linked cyber group "Shuckworm" is continuing to target Ukrainian organisations with info-stealing malware. Shuckworm is an eight-year-old cybercrime group that focuses almost exclusively on Ukraine. Much of the current activity is an extension of attacks that were reported by the Computer Emergency Response Team of Ukraine (CERT-UA) in July.[20]

Yet another threat actor, identified by Microsoft as SEABORGIUM, has been documented since 2017 actively conducting cyberespionage attacks against military personnel, government officials, think tanks, and journalists in Europe and the South Caucasus. The group abused the OneDrive service and fake LinkedIn accounts in campaigns that include persistent phishing, credential theft and data theft. On August 15, Microsoft announced a major disruption of this APT actor, cutting off access to accounts used for pre-attack reconnaissance, phishing, and email harvesting.[21]

Cisco Hacked by Ransomware Gang

On August 10, Cisco released a security incident notice and a technical blog post that revealed that an initial access broker with ties to the Russia-linked group UNC2447 used its employee's compromised credentials to gain access to the company's Virtual Private Network (VPN) and steal an alleged 2.8 GB of data through a series of "sophisticated voice phishing attacks" and compromising multi-factor authentication. The intrusion was detected on May 24, but the company shared the details in August after the cybercriminals published a list of files allegedly stolen from its systems. Cisco did not identify any impact to its business as a result of this incident, including on Cisco products or services, sensitive customer data or supply chain operations.[22]

Chinese Cyberspies Use Supply Chain Attack to Deliver Malware

On August 15, Cyber Security firm Trend Micro reported that the China-linked cyberespionage group "Iron Tiger" was observed using the compromised servers of MiMi – an instant messaging application available on Windows,

[19] Ukraine_ Ukraine nuclear operator reports cyberattack on its website, IT Security News, ET CISO.pdf
[20] Russia's Shuckworm cyber group launching ongoing attacks on Ukraine | TechRepublic
[21] Microsoft Announces Disruption of Russian Espionage APT | SecurityWeek.Com
[22] Cisco Hacked by Ransomware Gang, Data Stolen | SecurityWeek.Com

macOS, Android, and iOS – for malware delivery. Also referred to as APT27 and TG-3390 (Threat Group 3390), "Iron Tiger" has been active since 2010, targeting hundreds of organisations worldwide for cyberespionage purposes, mostly in Taiwan, including a Taiwanese gaming development company.[23]

China unveils its first quantum computer, 'Qianshi'

On August 24, Chinese search engine giant Baidu unveiled its first quantum computer named "Qianshi," joining the global race to apply the technology to practical uses. The Baidu-developed quantum computer, with a 10-quantum-bit (qubit) processor, has been made available to external users. The company has also developed a 36-qubit quantum chip.

Quantum computing is a form of high-speed calculation at extraordinarily cold temperatures that will exponentially enhance processing speeds. However, current real-world applications in the field are still very basic. Globally, governments and companies, competing for technology supremacy, will reportedly invest around $16.4 billion in quantum development by the end of 2027, according to market researcher IDC.[24]

Twitter's misleading regulatory disclosures alleged

On August 23, Peiter Zatko, Twitter's former head of security, in a whistle-blower complaint, accused the company of making misleading regulatory disclosures about spam and fake accounts. Zatko's allegations of widespread security failures and foreign state actor interference at Twitter raises serious concerns regarding data privacy and security risks for Twitter users around the world. These allegations are also likely to influence Elon Musk's effort to abandon a $44 billion takeover of Twitter.

In June, Twitter had responded to queries from Musk about how it calculates bots and whether an error in how it tallies monetisable daily active users (MDAU) revealed problems in its financial reporting. Peiter Zatko is to testify before the US Senate on September 13 on his allegations of security failures at the social network.[25]

[23] Chinese Cyberspies Use Supply Chain Attack to Deliver Windows, macOS Malware | SecurityWeek.Com
[24] China's Baidu reveals its first quantum computer, 'Qianshi' - Nikkei Asia
[25] Twitter whistleblower Peiter Zatko to testify in Congress - The Washington Post

US implements the CHIPS and Science Act of 2022

On August 9, the US President signed the CHIPS and Science Act of 2022, amid competitive concerns that China is moving ahead in producing chips needed for weapons systems and is gaining technology supremacy, which provided the rationale for subsidising US-based semiconductor manufacturing.[26] The law also restricts any recipient of the funds from expanding semiconductor production in China "or any other foreign country of concern". The Act earmarks nearly US$53 billion in semiconductor manufacturing incentives and another US$200 billion for research into artificial intelligence, quantum computing and other advanced technologies, all areas the Chinese government has designated as national priorities.[27] The CHIPs Act represents a fundamental paradigm shift in US policy regarding subsidising this strategic sector, and has spurred American companies to invest 'on shore' for semiconductor manufacturing.

The US is also restricting Chinese access to Western computer-chip technology through export controls, which some experts believe is one reason for Beijing's stepped-up militarism on Taiwan which manufactures the most advanced chips. To maintain supremacy in technology innovation, US R&D spending in 2020 was 3.5% of its GDP, as compared to 2.4% in China, according to the OECD.[28]

[26] FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China - The White House

[27] https://www.scmp.com/news/world/united-states-canada/article/3188336/biden-signs-law-authorising-us53-billion-subsidies

[28] The Semiconductor Boondoggle - WSJ

International Cooperation

India hosts Cyber Security Exercise "Synergy" for 13 countries

On August 31, the Indian Computer Emergency Response Team (CERT-In), in collaboration with Cyber Security Agency of Singapore (CSA), successfully designed and conducted a Cyber Security Exercise "Synergy" for 13 Countries as part of the International Counter Ransomware Initiative (CRI)[29]- Resilience Working Group, which is being led by India under the leadership of National Security Council Secretariat (NSCS).[30] Teams from each participating nation joined the exercise with the objective to assess, share and improve strategies and practices among Member-States to build network resiliency against ransomware and cyber extortion attacks. The exercise provided insights for better coordination and cooperation among CRI Member States.[31]

The US and Israel finalise MOU on Cyber Security Cooperation

On August 25, the United States and Israel announced the finalisation of a bilateral Memorandum of Understanding on Cybersecurity Cooperation to protect the integrity of the international financial system by collaborating on sharing information on incidents and threats, staff training in cybersecurity, and competency building activities such as the conduct of cross-border cybersecurity exercises.[32]

***

[29] Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021 - The White House.pdf- Counter ransomware initiative (CRI) involves 36 nations, that was formed after a meeting hosted by the US in October 2021.

[30] CERT-In conducts cyber security exercise 'Synergy' for 13 countries in collaboration with CSA Singapore, Government News, ET Government.pdf-- India leads the resilience working group vertical of CRI under NCSC. Australia, New Zealand, Japan, Singapore, and the United Kingdom were among 13 Countries who participated in the "Synergy".

[31] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1855771

[32] Israel: US inks agreement on Cyber Security Cooperation with Israel, IT Security News, ET CISO (indiatimes.com)

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

www.delhipolicygroup.org