Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

JULY 2021

Volume II, Issue 7 | July 2021

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

Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG Cyber Review
Vol. II, Issue 7
July 2021

ABOUT US

Founded in 1994, the Delhi Policy Group (DPG) is among India's oldest think tanks with its primary focus on strategic and international issues of critical national interest. DPG is a non-partisan institution and is independently funded by a non-profit Trust. Over past decades, DPG has established itself in both domestic and international circles and is widely recognised today among the top security think tanks of India and of Asia's major powers.

Since 2016, in keeping with India's increasing global profile, DPG has expanded its focus areas to include India's regional and global role and its policies in the Indo-Pacific. In a realist environment, DPG remains mindful of the need to align India's ambitions with matching strategies and capabilities, from diplomatic initiatives to security policy and military modernisation.

At a time of disruptive change in the global order, DPG aims to deliver research based, relevant, reliable and realist policy perspectives to an actively engaged public, both at home and abroad. DPG is deeply committed to the growth of India's national power and purpose, the security and prosperity of the people of India and India's contributions to the global public good. We remain firmly anchored within these foundational principles which have defined DPG since its inception.

DPG Cyber Review

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. II, Issue 7
July 2021

Contents

Abstract

The sixth anniversary of Digital India on July 1 had something to cheer about. Ranking way ahead of China and Pakistan, India secured 10th place in the ITU's Global Cybersecurity Index 2020. Notwithstanding the global ranking, India continues to face phishing attacks from cyber espionage groups from Pakistan and other adversaries. India is among the top three countries facing such attacks. The controversy over the IT Rules on Social media intermediaries seems to have subsided with the change of guard at the nodal ministry, as also compliance of the provisions by most tech platforms.

Early roll out of 5G network in India would need policy intervention for optimum spectrum auction and a conducive device eco-system suitable for multiple frequency bands.

On the international front, the revelations regarding Pegasus cyber surveillance, affecting 34 countries and including several world leaders, exposed the menace of unrestricted abuse of surveillance tools. This calls for global norms to bring about greater oversight and transparency.

The US has taken several measures to protect its domestic networks and critical infrastructure from cyber-attacks. These include diplomatic censure of China by the US and its allies, the issue of a National Security Memorandum for protecting critical infrastructure and a joint Cyber Security advisory detailing tactics, techniques and procedures (TTPs) used by Chinese state-sponsored threat actors.

With the continuing global chip shortage, geopolitics continue to drive the push for achieving self-sufficiency in semiconductor manufacturing and address supply chain vulnerabilities. New industrial policies are being initiated both by the west and China towards this end. China has also hardened its regulatory controls over its tech industry to fix certain anticompetitive practices and data security threats.

The UN Security Council held its first-ever open debate on maintaining peace and security in cyber space on June 29.

National Developments

India ranks 10th in Global Cybersecurity Index

Just ahead of the sixth anniversary of Digital India on July 1, the International Telecommunication Union (ITU), on June 29, published the Global Cybersecurity Index 2020 (GCI) that measures the commitment of its member states to cybersecurity. Ranking way ahead of China (at 33rd position) and Pakistan at (79th position), India jumped 37 places to rank 10th in the GCI, fourth among Asia-Pacific countries. The list is topped by the United States and followed by the United Kingdom and Estonia. Among India's neighbours, Bangladesh did well by jumping 25 notches up to rank 53 in the Index. The ranking is based on four pillars: legal measures, technical measures, capacity building measures and organisational measures. The latest ITU report will help secure digital ecosystems and address the growing cyber capacity gap between developed and developing countries by fostering knowledge, upskilling, and building competencies.[1] The improvement in India's ranking underscores the proactive role being played by the Computer Emergency Response Team (CERT-In) and other security agencies.

Cyber Threat Scenario in India

Notwithstanding the global ranking in the GCI, India is among the top three countries facing phishing attacks, primarily via instant mobile messaging apps like WhatsApp and Telegram. On July 22, the Indian Computer Emergency Response Team (CERT-In) identified close to 140 phishing incidents during the first half of 2021. CERT-In is working in coordination with service providers, regulators and law enforcement agencies (LEAs) to track and disable phishing websites and facilitating the investigation of fraudulent activities.[2]

Several such phishing attacks are being employed by a Pakistani cyber-espionage group, SideCopy, to target government and military establishments through spear-phishing emails with malicious file attachments that lure the user into extracting the attached zip archive.[3] A cyber espionage campaign by this group is also targeting high-profile PSUs from the telecom, power and finance sectors in India, a new report warned on July 13.[4]

[1] Global Cybersecurity Index 2020 - My ITU
[2] Nearly 140 phishing incidents observed by CERT-In during H1 2021, IT Security News, ET CISO (indiatimes.com)
[3] Pak group targets India's critical infrastructure, cybersecurity firm warns of phishing attack (aninews.in)
[4] https://www.nationalheraldindia.com/national/pak-based-hackers-targeting-critical-infrastructure-psus-in-india

Implementation of IT Rules 2021 by Social Media platforms

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have become fully effective from May 26, 2021, including for additional due diligence to be followed by Significant Social Media Intermediaries (SSMIs).

After the appointment of new ministers in the IT ministry, most major digital platforms, including Facebook, Google, LinkedIn and WhatsApp, have announced their compliance and have also started publishing a monthly compliance report. WhatsApp in its report on July 14, revealed that it banned over 29 lakh accounts between May 15 - June 15, 2021.[5] In its maiden report, Google reported that in June, it received 36,265 complaints from individual users, relating to third-party content that is believed to violate local laws or personal rights. One complaint may relate to multiple contents. Google removed 83,613 pieces of content, including copyright (83,054), trademark (532) and counterfeit (14). It also removed 5,26,866 contents in June from its platforms (including YouTube) by automated detection to enforce its guidelines and policies regarding harmful and violent extremist contents.[6]

However, Twitter was pulled up by the Delhi High Court on July 28 for non-compliance of the Rules regarding appointment of three key executives. Twitter currently faces lawsuits in several courts over content posted by third-parties on its platform.[7] To create an alternative to Twitter, many Indian government departments and ministers are promoting the indigenous micro-blogging platform 'Koo'.

Status of the roll out of 5G Networks

Currently, trials of 5G communications are being carried out by designated telecom operators. However, early roll out of 5G is dependent on several factors, as reported on July 27. One aspect of early roll out pertains to the device eco-system supporting multiple 5G frequencies, including all existing spectrum bands in the 3G and 4G bands. The rollout of 5G networks in multiple spectrum bands can only happen with the availability of compatible handsets. While chipsets are supportive of most of these bands, telecom operators have urged OEMs to provide the band support relevant for India as also for global 5G

[5] https://www.indiatoday.in/technology/news/story/whatsapp-banned-over-20-lakh-accounts-in-india-in-a-month-reveals-first-intermediary-guidelines-report-1828662-2021-07-15

[6] https://cio.economictimes.indiatimes.com/news/internet/google-says-it-removed-71132-content-pieces-in-may-83613-items-in-june-in-india/84889402

[7] https://telecom.economictimes.indiatimes.com/news/delhi-high-court-gives-twitter-last-opportunity-to-show-compliance-with-it-rules/84846739

frequencies.[8] However, adding these bands makes Radio Frequency (RF) more complex and adds to Bill of Material (BoM).

Optimum spectrum auction is another crucial aspect for early 5G rollout. Telecom operators are contesting allotment of potential 4G/5G spectrum for free to three global LEO satellite operators, OneWeb, Starlink and Amazon, on the premise of providing cheaper high-speed satellite-based internet services to rural and remote areas. In a letter to the telecom Secretary on July 5, Telecom Watchdog, a consumer forum and an NGO, warned that any move to give these satellite companies access to top-grade airwaves worth billions without auctions would flout a ruling of the nation's Supreme Court.[9]

The third crucial element would be the development of Radio Access Network (RAN) for the Indian environment. On July 20, Airtel announced collaboration with Intel for working towards 5G network development by leveraging Virtualised Radio Access Network (vRAN) and Open-RAN technologies. Simultaneously, Airtel has entered into a partnership with Tata Sons and Tata Consultancy Services to deploy O-RAN 5G solutions, including radio and core. Earlier, Reliance Jio had joined hands with Intel to help its 5G network development and test its homegrown solutions.[10]

Capability building on technologies and Cyber Security

The Government of India is committed to bring India to a leadership position in cyber security. With AI, cyber warfare, armed drones and standalone weapon systems now being part of warfare, the capability building for the armed forces has been taken up in full earnest.

It was reported on June 30 that the US, under the 2016 India-US Cyber Framework and defence cooperation agreement, has offered to train up to 100 military personnel in the Silicon Valley to give them first-hand experience on how to counter cyber warfare and AI roles in future defence and warfare.[11]

The Indian Navy inked a MoU with the DPSU Bharat Electronics Limited on June 29 to develop emerging technologies related to artificial intelligence, quantum computing and robotics. The MoU provides for the setting up of a

[8] 5G Smartphones: 5G band support: Smartphone makers say in line with Indian telcos' network strategy, Telecom News, ET Telecom (indiatimes.com)
[9] OneWeb: Telecom Watchdog asks DoT to stop OneWeb, Starlink and Amazon from getting free 5G spectrum through backdoor, Telecom News, ET Telecom (indiatimes.com)
[10] https://telecom.economictimes.indiatimes.com/news/after-jio-intel-lands-new-o-ran-5g-network-deal-with-airtel/84611108
[11] Indian military personnel to train in US on cybersecurity, command in the offing | Latest News India - Hindustan Times

technology incubation forum to jointly work on developing new technologies.[12]

Further, as part of capability building, the Indian Institute of Technology, Kanpur (IIT-K) on July 23, launched the first technology innovation hub to find cyber security solutions for anti-drone technologies, intrusion detection system, block-chain and cyber physical system. As many as 13 start-ups and 25 research and development principal investigators were selected after a rigorous application process. The start-ups, supported by the Interdisciplinary Centre for Cyber Security and Cyber Defence of Critical Infrastructures (C3i Centre) at IIT Kanpur, will innovate to prevent disruption of the cyber security space, focusing on design and development of services and products to safeguard India's critical infrastructure.[13]

Experimentation of CBDC by RBI

The Reserve Bank of India is working toward a phased implementation strategy on a Central Bank Digital Currency (CBDC), as announced by the RBI deputy governor on July 22. A CBDC is a form of cryptocurrency that is backed by sovereign reserves. Unlike private crypto assets like Bitcoin or Ethereum, the value of these digital coins is not subject to volatile market fluctuations. The RBI is examining several aspects including the scope, technology, validation base and distribution format. It is also considering an enabling legal framework. A pilot project to test a general-purpose digital currency is planned.[14] With this, India joins China, Russia and the UK among major economies evaluating the issuance of the Central Bank Digital Currency.

[12] Indian Navy signs pact with Bharat Electronics Ltd to develop emerging technologies, IT News, ET CIO (indiatimes.com)
[13] IIT-K launches technology innovation hub to find cyber security solutions for anti-drones technologies, IT Security News, ET CISO (indiatimes.com)
[14] RBI is working on making virtual currency a reality - The Economic Times (indiatimes.com)

International Developments

Global abuse of Cyber Surveillance tools

The unlawful abuse of cyber surveillance tools is presenting privacy and human rights challenges globally. On July 18, the French non-profit 'Forbidden Stories' and human rights organisation 'Amnesty International' revealed a list of phone numbers purportedly targeted for surveillance by the cyber tool Pegasus, sold worldwide by the Israeli company NSO. These organisations shared the sensational list with 17 media publications, including The Wire, The Guardian and The Washington Post. While Forbidden Stories organised the media consortium's investigation, titled the 'Pegasus Project', Amnesty International provided analysis and technical support. The leaked unauthenticated database of 50,000 names, which includes 300 numbers in India, is raking up a storm across the world because it includes the mobile phone numbers of business executives, human rights activists, journalists and a number of diplomats, military chiefs and senior politicians from 34 countries, including the French president, Emmanuel Macron, the South African president, Cyril Ramaphosa, and the Pakistani prime minister, Imran Khan. Investigations have been instituted by France, Hungary and Israel while Morocco has filed a defamation suit against these organisations. On July 29, the Jerusalem post reported that Israeli defence investigators raided the NSO Group's Herziliya office, near Tel Aviv. The company currently holds a license from the Israeli government for the sale of surveillance tools to foreign government organisations for lawful interceptions[15].

In India, the controversy has generated political turmoil both inside and outside parliament. While opposition parties, dissatisfied with the denial by the government of any unlawful activity, are demanding investigation under the Supreme Court, several entities have sought recourse to legal remedies[16]. Notwithstanding the claim of the NSO Group that it develops tools that allow governments to pursue criminals and terrorists, the spectre of unrestricted surveillance calls for global norms with greater oversight and transparency.[17]

US takes several measures on Improving Cybersecurity

Following a series of cyberattacks on its critical infrastructure and domestic networks, the US has announced several diplomatic, political and technical

[15] https://www.jpost.com/breaking-news/israeli-govt-representatives-visit-nso-headquarters-675185
[16] https://www.indiatoday.in/law/story/pegasus-row-sc-agrees-to-hear-plea-seeking-independent-inquiry-into-snooping-allegations-1834570-2021-07-30
[17] Emmanuel Macron identified in leaked Pegasus project data | France | The Guardian

measures. In a statement on July 19, the White House publicly accused China of using "criminal contract hackers", affiliated to its intelligence agencies, who carry out both state sponsored activities and cybercrime for their own financial gain. This was part of a global censure in which the US and its allies, including the European Union, the U.K., Canada, Australia, New Zealand, Japan and the North Atlantic Treaty Organisation (NATO) held the People's Republic of China (PRC) accountable for its pattern of irresponsible, disruptive, and destabilising behaviour in cyberspace, which poses a major threat to their economic and national security. It blamed the hackers tied to China's Ministry of State Security (MSS) for the indiscriminate hack of Microsoft Exchange Server software that emerged in March, which rendered an estimated hundreds of thousands of mostly small businesses and organisations vulnerable to cyber intrusion.[18] Chinese diplomatic missions in five countries and the European Union denounced the US allegations as a political conspiracy lacking in evidence.[19]

Concurrently, US security agencies - the NSA, FBI and the DHS's Cybersecurity and Infrastructure Security Agency (CISA) - released a joint advisory on July 19, detailing more than 50 tactics, techniques and procedures (TTPs) used by Chinese state-sponsored threat actors in their attacks. This Joint Cybersecurity Advisory (CSA) recommends technical measures for detection and mitigation, as well as defensive tactics and techniques.[20]

Further on July 28, the White House issued a National Security Memorandum on Improving Cybersecurity for Critical Infrastructure to prevent the degradation, destruction, or malfunction of industrial control systems that could cause significant harm to the national and economic security of the United States. The memorandum calls for exchange of threat information for priority control systems in critical infrastructure. Cyber security performance goals for critical infrastructure will be measured to further a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety.[21]

[18] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

[19] China rejects Microsoft Exchange cyber hacking charge, accuses US of 'massive' eavesdropping | South China Morning Post (scmp.com)

[20] https://us-cert.cisa.gov/ncas/alerts/aa21-200b

[21] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

Additionally, the U.S. Department of State's Rewards for Justice (RFJ) program is offering a reward of up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, participates in malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA). Violations of the statute may include transmitting extortion threats as part of ransomware attacks, intentional unauthorised access and intentionally causing damage without authorisation to a protected computer. This includes not only U.S. government and financial institution computer systems, but also those used in or affecting interstate or foreign commerce or communication. The Rewards for Justice program has set up a Dark Web (Tor-based) tips-reporting channel to protect the safety and security of potential sources. Reward payments may include payments in cryptocurrency.[22]

Saudi Oil Company faces ransomware attacks

The oil and gas industry, which includes companies that own wells, pipelines and refineries, has long been a laggard in cyber security spending. The Middle Eastern oil major, Saudi Aramco, confirmed on July 21 that some company files were leaked after hackers reportedly demanded a $50 million ransom from the oil producer. The files apparently came from one of its contractors. Aramco said that the extortionists possibly held 1 terabyte worth of Aramco data.[23]

Continuing Geopolitics over Chip shortage

The global chip shortage has put semiconductor production in the spotlight like never before. Governments in the US, EU and Asian chip producing countries have embarked on measures to achieve self-sufficiency in semiconductor manufacturing and address supply chain vulnerabilities.

It was reported on July 29 that an industrial policy to offer subsidies to industries critical to national interest, long criticised by western nations as inefficient, is being adopted.[24] Last month, the U.S. Senate voted for direct industry subsidies worth $52 billion for new semiconductor fabrication plants, called "fabs." The European Union has committed to nearly doubling its share of global semiconductor manufacturing capacity, to 20%. South Korea approved up to $65 billion in support for semiconductors, and Japan promised

[22] https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-foreign-malicious-cyber-activity-against-u-s-critical-infrastructure/
[23] https://www.aljazeera.com/economy/2021/7/21/saudi-aramco-confirms-data-leak-after-reports-of-cyber-ransom
[24] https://www.wsj.com/articles/subsidies-chips-china-state-aid-biden-11627565906

to match other countries' semiconductor subsidies while planning to turn Japan into an Asian data center hub. Not to be outdone, China announced the "dual circulation" policy last year, to eliminate China's dependence on other countries while increasing their dependence on China.[25]

Consolidation has also swept through the semiconductor industry to upscale and expand product portfolios. Taiwan Semiconductor Manufacturing Co. (TSMC), the world's largest contract chip maker, is to invest $100 billion over the next three years. TSMC is already setting up a massive state-of-the art manufacturing plant in southern Taiwan to produce 5-nanometer processors. Samsung Electronics Co. plans to invest about $116 billion by 2030 to diversify and boost its semiconductor output, and is considering an investment of up to $17 billion to build a new chip-making factory in the U.S. On July 17, the Wall Street Journal reported that Intel is considering the acquisition of GlobalFoundries (GF) at roughly a $30 billion valuation. GF reportedly occupies the 4th position in foundry business with about 7% market share. It has fabs in the US, Germany and Singapore for manufacturing legacy chips with up to 12nm technology. GF also has an office in Bengaluru, India from where it supports IT, fab operations, design to mask as well as characterisation and modelling. Like Intel and TSMC, GlobalFoundries itself is expanding its manufacturing footprint, by investing more than $4 billion on a new chip-production facility in Singapore.[26]

In the entire value chain, a high-end chip production machine made by ASML Holding in the Netherlands reportedly holds the trump card. This machine uses lasers and mirrors to draw lines to define ultra-small circuitry on chips. The Dutch government has so far been persuaded to deny its sale to China by successive US governments. Reports speculate that the spectre of semiconductor dominance could provide China an added incentive to move on Taiwan, and the U.S. an added incentive to stop China from doing so.[27]

China drafts new cyber-security industry plan

On July 12, China's Ministry of Industry and Information Technology issued a draft three-year action plan to develop the country's cyber-security industry, estimating the sector may be worth more than 250 billion yuan ($38.6 billion) by 2023. The plan states that changes in security related to 5G, cloud computing and AI technologies have raised the bar for protection of digital assets. It will increase the number of cybersecurity graduates and widen coverage of

[25] https://www.wsj.com/articles/subsidies-chips-china-state-aid-biden-11627565906
[26] Intel Is in Talks to Buy GlobalFoundries for About $30 Billion - WSJ
[27] The Really Critical Infrastructure Need: American-Made Semiconductors - WSJ

industries that deal with modern technologies. The integration and innovation of emerging technologies and cybersecurity will accelerate significantly.[28]

China tightens regulatory measures on Tech Companies

Continuing with its recent regulatory drive, on July 26 China's Ministry of Industry and Information Technology introduced a new six-month rectification program aimed at correcting a range of industry issues, including disrupting market order, infringing on users' rights and mishandling user data. This program will regulate the country's internet giants to fix certain anticompetitive practices and data security threats. The regulation includes self-examination and rectification, gathering information and strengthening legal enforcement and accountability.

In June, China enacted a sweeping Data Security Law that mandates companies to obtain approval from law enforcement agencies to transfer data stored in China to overseas entities. The law takes effect on September 1; violators will be fined up to $1.5 million and could have their business suspended.[29]

Another regulatory action on companies engaged in online/in- person private tutoring, online financial services and other sectors was announced on July 26. This fuelled a crash in the shares of these companies. After the market rout, the vice chairman of the China Securities Regulatory Commission held a meeting on July 29 to reassure banks and investors. It was emphasised that China has no intention to decouple from global markets, and especially from the U.S.[30]

[28] https://www.globaltimes.cn/page/202107/1228461.shtml
[29] https://www.wsj.com/articles/chinas-tech-regulator-orders-companies-to-fix-anticompetitive-security-issues-11627304021
[30] https://www.wsj.com/articles/china-moves-to-reassure-global-banks-and-investors-after-market-rout-11627528509

International Cooperation

First-Ever Debate on Cyberthreats at the UNSC

Coinciding with the International Telecommunication Union's release of the global cybersecurity index on June 29, the UN Security Council held its first-ever open debate on maintaining peace and security in cyber space. The virtual meeting was presided over by the Prime Minister of Estonia, as the President of UNSC for June, with the participation of senior officials from various capitals. The consensus outcomes of the Group of Governmental Experts and the Open-Ended Working Group on cyber security had encouraged such a debate. Opening the discussion, the United Nations High Representative for Disarmament Affairs said that the explosive growth of digital technologies is creating a new potential for conflict. He pointed to a dramatic surge in malicious incidents in recent years, contributing to diminishing trust and confidence among States. Particularly at risk is critical infrastructure - including financial institutions, health-care facilities and energy grids. The political and technical difficulties in attributing and assigning responsibility for ICT attacks could result in significant consequences, including unintended armed responses and escalation. These dynamics can encourage States to adopt offensive postures for the hostile use of these technologies.

In the debate that followed, representatives on the 15-member Council emphasised that cyberspace is subject to international law, including the Charter of the United Nations and the principle of State sovereignty. The Indian Foreign Minister stated that Member States must adopt a collaborative rules-based approach in cyberspace and work towards ensuring its openness, stability and security.[31]

[31] https://www.un.org/press/en/2021/sc14563.doc.htm

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

www.delhipolicygroup.org