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

DPG CYBER REVIEW

JUNE 2022

Volume III, Issue 6 | June 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 6
June 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

© 2022 by the Delhi Policy Group

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

DPG Cyber Review
Vol. III, Issue 6
June 2022

Contents

Abstract

India's cyberspace was targeted by hackers based in Malaysia, Yemen, Pakistan and other countries, accompanied by a sustained disinformation campaign on social media, following derogatory remarks against Prophet Mohammad made by certain BJP functionaries. Instances of violation of the Intermediary Guidelines and Digital Media Ethics Code (IT Rules, 2021) by Twitter and other platforms, on content take-down notices, were a matter of concern to the Indian authorities.

To meet the challenges of cyber criminals, the Indian Government barred its employees from using third-party virtual private networks (VPN) and app-based scanner and anonymisation services. Suggestions for accountability of technology providers were also made by India at the meeting of the UN Open-Ended Ad Hoc Committee of Experts to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes.

While the approval of a 5G spectrum auction by the Union Cabinet was welcomed, its ruling on direct allotment to enterprises for private networks has generated a rift between telecom operators and technology companies. The spectrum in the 700 MHz band, long ignored for 4G spectrum auction by telecom operators, is likely to be assigned for railway communications to prevent economic loss to the nation.

India has stepped up efforts to become a major investment destination for semiconductors, and will reportedly spend some $30 billion to overhaul its tech industry and build up a chip supply chain.

Notwithstanding a perceptible ineffectiveness of cyber warfare in the ongoing kinetic battle in Ukraine, a report released by Microsoft during the month cited disruptive activities by Russia against Ukraine since the commencement of hostilities on February 24.

The US and the EU are trying to forge an alliance with Taiwan to reinforce a 'silicon shield' against Chinese aggression.

China has sought public comments on a proposed regulation that would require social media platforms to review every single post and comment by users before publishing.

The XIV BRICS Summit recognised the potential of ICT for growth and development, while expressing concern at the rising level and complexity of criminal misuse of ICT. Leaders of the G-7 launched a "Partnership for Global

Infrastructure (PGII)" and pledged $600 million for a submarine telecommunications cable connecting Singapore to France.

National Developments

National Cyberspace scenario

Amidst public protests against and denouncement of remarks on Prophet Mohammad made by certain BJP functionaries, several websites in India were targeted by hackers based in Malaysia, Yemen, Pakistan and other countries.

On June 12, the website of a prominent academic institution was defaced by 'DragonForce Malaysia', whose message on its home page urged people to unite and start a campaign against India. Additionally, the Yemeni 'Cyber Army' claimed to have defaced over 1,200 Indian sites, while 'Team Revolution-Pakistan' compromised live news streaming services.[1] Hacker groups like 'D4RKTSN' and 'Zerofault' defaced more than 250 websites over three days.[2]

Indian cyber space was also a target of a sustained disinformation campaign. On June 11, a report by the Digital Forensics Research and Analytics Centre (D-FRAC) detailed how Pakistan-based Twitter handles were exclusively created to spread false narratives in India on this sensitive issue. These handles started tweeting content with hashtags that soon started trending on Twitter, thereby creating an impression that the entire Gulf region was united in anger against India, which pushed the governments of the respective countries to issue statements against India.[3] Instances of violation of the Intermediary Guidelines and Digital Media Ethics Code (IT Rules, 2021) were observed. Twitter and some other significant social media intermediaries failed to act on the content take-down notices sent under Section 69A of the IT Act.[4] On June 27, the IT ministry issued a notice to Twitter to comply with the country's IT Rules by July 4 or risk losing its immunity as an intermediary. The National Cyber Security Strategy, which is expected to bring a focused approach to all aspects of cyber security including curbing disinformation and data protection, meanwhile still remains a work in progress.

India also continues to be the sixth largest target of cyber criminals. More than 1.1 m. complaints, including 0.2 m. complaints of social media crimes, have been registered on the cybercrime reporting portal. On June 21, the Indian Home Minister cautioned that threats to cyber security are posing major risks

[1] 72 Hours On, Hackers Continue To Deface Govt & Private Sites, IT Security News, ET CISO (indiatimes.com)

[2] Nagpur's Institute of Science's Website Targeted by Malaysian Hackers, Restoration in Progress | Technology News (gadgets360.com)

[3] https://www.sundayguardianlive.com/news/india-moves-counter-disinformation-warfare

[4] Twitter: MeitY flags lack of response from Twitter to notices, Telecom News, ET Telecom (indiatimes.com)

to national security. The government is upgrading capability to deal with these threats, and MHA has established a Indian Cyber Crime Coordination Center (I4C) to fight against cybercrimes.[5]

India bans VPN, cloud services for government employees

On June 16, the Indian Government barred its employees from using third-party virtual private networks (VPN) and anonymisation services, which are exploited by cyber criminals. The directive also urged government employees not to save any "internal, restricted or confidential government data files" on any non-government cloud service such as Google Drive or Dropbox, and prohibited use of external mobile app-based scanner services such as the Chinese 'CamScanner' to scan "internal government documents."[6]

These guidelines have been issued just days after global VPN companies, including ExpressVPN, Surfshark and NordVPN, said they would stop operations in India and offered users connections to virtual Indian VPN servers based in Singapore and the UK.

Earlier on April 28, the Indian Computer Emergency Response Team (CERT-In) had issued a set of guidelines that require companies providing VPN services to keep a log of their users for five years. They are also to store information such as username, email ID used while signing up, contact numbers and internet protocol addresses. The rules were slated to be effective on June 26, but a notification on June 28 has extended the deadline till September 25.[7]

India calls for Countering use of technology for cybercrime

In line with its domestic regulation, at the meeting of the UN Open-Ended Ad Hoc Committee of Experts held in Vienna from May 30- June 10, India proposed a comprehensive international convention on countering the use of ICTs for criminal purposes, raising a warning against the anonymity offered to criminals and terrorists by technologies, and the increasing possibility of their remaining untraceable to law enforcement agencies. India also sought global action to counter the use of technologies including virtual private networks (VPN), end-to-end encrypted messaging services and blockchain-based

[5] Cybersecurity linked to national security, India upgrading to take on threat: Amit Shah | India News,The Indian Express

[6] vpn: Govt bans VPN, cloud services for employees, IT Security News, ET CISO (indiatimes.com)

[7] Government extends deadline to comply with new cybersecurity rules | Latest News India - Hindustan Times

technologies such as cryptocurrency. It further suggested a cooperation framework for "freezing and return" of proceeds obtained from cybercrime.

This multilateral Committee was established by a UNGA resolution in January 2020, to discuss and decide on developing an international convention with universal acceptance to counter global cybercrime.[8]

5G Spectrum auction approval generates controversy

On June 15, the 5G spectrum auction was approved by the Union Cabinet, paving the way for the issue of the Notice Inviting Applications (NIA) on the same day. The auction is set to take place from July 26, with the possibility of 5G rollout in August. The approval provides enterprises the option of obtaining spectrum directly from the DoT to develop their private 5G networks based on specialised and distinctive captive use. This has generated a rift between telecom operators and technology companies.

The Cellular Operators Association of India (COAI), representing telecom operators, contended that taking away chunks of crucial spectrum for private enterprises would fragment available spectrum and threaten the wider success of 5G, posing a threat to national security.[9]

On June 18, it requested the government to provide a level-playing-field, with equitable license fees and restricting the scope of such non-public networks to machine to-machine communication inside specific premises. Operators have also called on the telecom department to ensure that captive private networks are set up strictly by enterprises and not by system integrators, failing which the latter would gain a backdoor entry into telecom services.[10]

The Broadband India Forum, representing technology companies, hailed the Union Cabinet's decision as a facilitator for digital transformation. Tata Consultancy Services (TCS) cited the example of countries such as Germany, Finland, UK, US, France, Sweden, South Korea, Hong Kong, Malaysia, Australia, Czech Republic, Japan and Taiwan which have earmarked spectrum for private networks in the mid band (3.3-3.67 GHz) and millimetre wave (28 GHz) band.

Telecom operators are likely to use 4G core to offer 5G services (non-standalone configuration) in the near term, and may skip bidding of spectrum

[8] India Urges World to Act on Use of VPN, Crypto, Encryption for Terror - The Economic Times.pdf

[9] 5G private networks_ COAI disappointed on captive network decision; seeks level playing field for orderly growth, Telecom News, ET Telecom.pdf

[10] 5G private networks: Don't allot 5G spectrum to system integrators, intermediaries: Telcos to DoT, Telecom News, ET Telecom (indiatimes.com)

in the 700 MHz band. To prevent economic loss to the nation, a consultation paper was floated by the Telecom Regulatory Authority of India (TRAI)[11] on June 9 on reserving the spectrum requirements in this band for State railway organisations such as the National Capital Region Transport Corporation (NCRTC) along with the Indian Railways, for the development of the ecosystem for Railway Radio-communication Systems between Train and Trackside (RSTT).[12]

India steps up as a chip investment destination

The potential of India as a semiconductor manufacturing destination, in view of the geopolitical uncertainty and supply chain concerns, is being increasingly recognised. Many semiconductor companies have research and development centres in India, so it is only logical for these centres to be supported by fabrication companies.[13]

On June 16, the Director-General of the India-Taipei Association announced that India will spend $30 billion to overhaul its tech industry and build up a chip supply chain to ensure it is not "held hostage" to foreign providers.[14] The investment initiative is aimed at increasing local production of semiconductors, displays, advanced chemicals, networking and telecom equipment as well as batteries and electronics. Experts believe that investments in India and Southeast Asia will flow as manufacturers adopt the 'China plus one' strategy.

Army signs pact with IIT-Madras for 5G testbed project

To foster capacity development, on June 21, the Indian Army partnered with IIT-Madras to establish a 5G Testbed at the Military College of Telecommunication for the army's operational use of 5G technology. A memorandum of understanding (MoU) to this effect calls for the institutions to collaborate on research and prototype development on 5G-enabled future communications.[15]

[11] https://www.trai.gov.in/consultation-paper-spectrum-requirements-national-capital-region-transport-corporation-ncrtc-train

[12] https://www.communicationstoday.co.in/dot-may-consider-assigning-700-mhz-spectrum-to-railways-if-operators-dont-bid/

[13] India touted as chip investment alternative amid regional risks - Nikkei Asia

[14] India to pump $30bn into tech sector and chip supply chain - Nikkei Asia

[15] 5G testbed_ Army signs pact with IIT-Madras for 5G testbed project for use at borders, CIO News, ET CIO.pdf

International Developments

Cyber activities and the Russia-Ukraine conflict

Notwithstanding perceptible ineffectiveness of cyber operations in the predominantly kinetic conflict, there have reportedly been several cyber-attacks by Russians against Ukraine since the commencement of hostilities. On June 22, a Microsoft report on "Defending Ukraine: Early Lessons from the Cyber War" concluded that Ukraine's cyber defences have shown resilience against destructive Russian cyberattacks on Ukrainian agencies and enterprises in the early phases. The Russian cyberattack on a satellite-communications company Viasat, which took down internet service for thousands of Ukrainians and Europeans, was effectively restored with the induction of 'Starlink' Satellite systems.

The report also cites Russian "strategic espionage" against governments, think tanks, businesses and aid groups in 42 countries supporting Kyiv. The United States was the prime target along with Poland, the main conduit for military assistance flowing to Ukraine. These attempts were thwarted by proactive measures.

To fight against alleged Russian disinformation and propaganda, Ukraine is being helped with training and tools by members of the EU, NATO and some private companies.[16] On June 14, it was reported that Ukraine has moved sensitive data, possibly to Poland, France and Estonia. It is also negotiating with other European nations for further data migration.

US President Signs Two Cybersecurity Bills into Law

On June 21, the US President signed the the Federal Rotational Cyber Workforce Program Act of 2021, and the State and Local Government Cybersecurity Act of 2021.

The Federal Rotational Cyber Workforce Program Act proposes a program under which certain federal employees can be temporarily moved to other agencies to boost their skills. Agencies can determine whether a position involving IT or cybersecurity is eligible for the program. The State and Local Government Cybersecurity Act of 2021 is meant to improve collaboration between the Department of Homeland Security and state, local, tribal and territorial governments. The bill requires the National Cybersecurity and Communications Integration Center (NCCIC) to coordinate with the Multi-

[16] Ukraine Has Begun Moving Sensitive Data Outside Its Borders - WSJ

State Information Sharing and Analysis Center (MS-ISAC) for cybersecurity exercises, training, and education and awareness.[17]

Earlier on May 12, President Biden had issued an Executive Order on Improving the Nation's Cybersecurity (EO 14028) to implement a set of requirements for operations and procurement.[18] The Executive Order aims to enhance software supply chain security, establish a Cyber Safety Review Board (Board) and adopt National Security Systems.

China-Backed Hackers Breached Global Telecom Firms

On June 12, the US Cybersecurity & Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI) issued a joint advisory regarding a cyber-espionage campaign by Chinese government-backed hackers. These hackers are said to have broken into several major telecom businesses throughout the world, gaining access to their targets by exploiting severe vulnerabilities in common networking devices.

The group used sophisticated techniques to acquire critical private information from technology and manufacturing organisations in the US, Europe and Asia.[19]

Taiwan's chips act as "silicon shield" against Chinese aggression

It was reported on May 31 that China had imported $350 billion worth of semiconductors in 2020, more than the value of the crude oil it imported in the same year.[20] An op-ed in Nikkei Asia of May 30 observed that Taiwan's chips are its "silicon shield" against Chinese aggression and a conflict would hit China's economy hard.

The US and the EU are trying to forge an alliance with Taiwan to reinforce this 'silicon shield'. On June 2, the annual EU-Taiwan Trade and Investment Dialogue (TID) was held, in which both sides focussed on supply chain resilience considering the Ukraine war and COVID-19 pandemic.[21] Earlier on March 29, the US had proposed forging a semiconductor industry alliance with Taiwan, South Korea and Japan to counter China in this strategic sector.

[17] Biden Signs Two Cybersecurity Bills Into Law | SecurityWeek.Com

[18] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[19] China-Backed Winnti Group Behind Major Cyber Espionage, Finds Israel-American Firm (news18.com)

[20] Sanction semiconductors to deter China's Taiwan ambitions – China Vs Taiwan

[21] https://policy.trade.ec.europa.eu/news/eu-and-taiwan-hold-trade-and-investment-dialogue-2022-06-02_en

However, these countries are not fully on board, as China's market is of paramount importance to them.[22] South Korea is struggling to break its dependence on Japanese chipmaking materials, including hydrogen fluoride, photoresist and fluorinated polyamides, a sign that political rhetoric alone is not enough to reshape supply chains. There is thus a shared commitment to maintaining the status quo in the Taiwan Strait.[23]

China plans to review each social media comment

On June 24, the Cyberspace Administration of China (CAC) sought public comments on a proposed regulation that would require social media platforms to review every single post and comment by users before publishing. The proposed regulation directs platforms to hire a content moderation team to review all user comments and filter out "harmful" ones before publishing. All types of comments including "bullet chats" that appear on top of a video fall under its purview. The draft also proposes that the originator who uploads a post is also responsible for the comments made by others.[24]

Chinese supercomputer achieves 'brain-scale' AI model

It was claimed on June 22 that Chinese scientists have successfully run an artificial intelligence model called "bagualu", meaning the "alchemist's pot". The model, with 174 trillion parameters, is on a par with the US 'Frontier', considered the world's most powerful supercomputer. Named the 'Sunway', it resembles a powerful human brain with its speed of a billion operations per second, more than 37 million CPU cores, nine petabytes of memory and 96,000 semi-independent computer systems called nodes. Potential uses include autonomous vehicles and facial recognition, as well as natural language processing, computer vision, life sciences and chemistry.[25]

[22] US plans semiconductor alliance with Taiwan, South Korea, and Japan – ThePrint – ANIFeed

[23] Sanction semiconductors to deter China's Taiwan ambitions - Nikkei Asia.pdf

[24] China plans to review every single social media comment, sparking more censorship fears | South China Morning Post (scmp.com)

[25] China supercomputer achieves global first with 'brain-scale' AI model | South China Morning Post (scmp.com)

International Cooperation

XIV BRICS Summit Beijing Declaration

On June 23, the Fourteenth BRICS Summit was held to "Foster High-quality BRICS Partnership", at which the leaders declared that the task of strengthening and reforming the multilateral system also encompasses the use of innovative and inclusive digital and technological tools. Technologies are required to better respond to new and emerging, traditional and non-traditional challenges, including those emanating from terrorism, money laundering, the cyber-realm, infodemics and fake news.

The BRICS leaders recognised the potential of ICTs for growth and development, while expressing concern at the rising level and complexity of criminal misuse of ICTs. They welcomed the ongoing work in the UN Open-Ended Ad Hoc Committee of Experts to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes and reaffirmed commitment to cooperating in the implementation of the mandate adopted by the UN General Assembly resolution 75/282.[26]

U.S. and G-7 Allies Detail Infrastructure Plan to Challenge China

On June 26, the US and G-7 allies launched the "Partnership for Global Infrastructure (PGII)" to close the infrastructure gap in developing countries, strengthen the global economy and supply chains, and challenge China's dominance. It was announced that the U.S. would contribute $200 billion over five years toward the Partnership for Global Infrastructure and Investment, including a $2 billion solar project in Angola and a $600 million submarine telecommunications cable connecting Singapore to France. The US aims to mobilise $600 billion for PGII by 2027 for global infrastructure investments.

The G-7 infrastructure projects will focus on investments in climate resilience, secure information and communications technology, gender equity and modernising health systems, including vaccine manufacturing facilities, to counter China's influence in developing nations through its Belt and Road Initiative and Digital Silk Road projects.[27]

[26] https://www.mea.gov.in/bilateral-documents.htm?dtl/35435/XIV_BRICS_Summit_Beijing_Declaration

[27] FACT SHEET: President Biden and G7 Leaders Formally Launch the Partnership for Global Infrastructure and Investment | The White House

India-Bangladesh Bilateral Cooperation

On June 19, India and Bangladesh foreign ministers met for the 7th Joint Consultative Commission meeting and decided to expand the bilateral strategic partnership to develop cooperation in areas of Artificial Intelligence, cyber security, startups and Fintech, besides expanding ties in the railways sector as well as cross-border river management and conservation. India and Bangladesh are also to work together in areas like start-ups, cyber security and Interoperable Digital Payment System (IDPS).[28]

***

[28] 7th round of India-Bangladesh Joint Consultative Commission: Looking forward to working on new areas of cooperation, says Jaishankar | India News,The Indian Express

DPG

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

www.delhipolicygroup.org