Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

MAY 2022

Volume III, Issue 5 | May 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 5
May 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 5
May 2022

Contents

Abstract

India experienced over 18 million cyber-attacks and threats in the first quarter of 2022. The attacks included ransomware, deepfakes and cryptocurrency-related scams to target financial and critical sectors.

To realise India's vision to become a thriving semiconductor hub, a number of semiconductor R&D programs, in collaboration with industry and academia, have been launched. India is also collaborating with its Quad partners under the "Semiconductor Supply Chain Initiative".

A 5G Test Bed has been launched as a multi-institute collaborative project, that will allow start-ups and industry players to test their products, prototypes and algorithms. Recommendations of the 5G spectrum auction await Cabinet approval.

"Cyber Security Directives 2022" issued by CERT-In have evoked a mixed response from industry, mainly due to operational challenges.

The Army Training Command, in collaboration with Rashtriya Raksha University (RRU), an institute under the Ministry of Home Affairs (MHA), has launched a "Wargame Research and Development Centre", that will use artificial intelligence (AI) to design virtual reality wargame training modules, for the Army to test strategies.

India has proposed holding a special meeting of the UN Security Council's Counter-Terrorism Committee (CTC) in India, to discuss ways to tackle the implications of terrorist exploitation of digital technologies.

BRICS Ministers reaffirmed their commitment to a secure ICT-environment and welcomed the ongoing work in the UN Open-Ended Ad Hoc Committee of Experts to draft a comprehensive international convention on countering the use of ICTs for criminal purposes.

Leaders of the Quad countries recognised the urgent need for a collective approach towards enhancing cybersecurity, the defence of critical information infrastructures, resilience of supply chains for digitally enabled products and services, and aligning baseline software security standards.

National Developments

Attacks on India's Cyberspace

On May 4, a report by the cyber security firm Norton revealed that India experienced over 18 million cyber-attacks and threats in the first quarter of 2022, which included nearly 60,000 phishing attempts and over 30,000 technical support scams. Multiple tactics, including "Deepfakes" that were linked to trending events and cryptocurrency-related scams, were used against critical and financial sectors.[1]

On May 19, the Indian Computer Emergency Response Team (CERT-In), issued a high severity warning for users of Apple iPhone, Apple Watch, Apple TV and Apple MacBooks. Multiple vulnerabilities were reported, exploiting which threat actors can bypass security restrictions to execute codes and control another device remotely. Apple apprehends that these vulnerabilities may have already been exploited by hackers. CERT-In, in its advisory, has urged mobile device users to implement software updates as soon as possible.[2]

India proposes UNSC CTC meeting to address technology challenges

Recognising that international collaboration is required to address cyber threats posed by terrorists, India on May 23 proposed holding a special meeting of the UN Security Council's Counter-Terrorism Committee (CTC) in India, which will discuss ways to tackle exploitation of digital technologies by terrorists. India's Permanent Representative, speaking at a UNSC briefing on "The Use of Digital Technologies in Maintaining International Peace and Security", highlighted the dangers from terrorist exploitation of new financial technologies including virtual currencies, nonfungible tokens (NFTs) that create monetary value out of non-physical entities, and crowd-funding platforms etc. and urged member states to address these challenges more strategically. The establishment of the UN Ad Hoc Committee to elaborate a Comprehensive International Convention on countering the use of information communication technology for criminal purposes was welcomed by India as a step in the right direction.[3]

[1] https://www.outlookindia.com/business/norton-prevented-more-than-18-million-cyber-attacks-in-q1-2022-in-india-news-195040
[2] Cert-IN now issues high severity warning for users of Apple iPhone and all its products; 'update urgently', Government News, ET Government (indiatimes.com)
[3] Welcome to Permanent Mission of India to the UN , New York (pminewyork.gov.in)

Industry driven Semiconductor Research initiated by India

To realise India's vision to become a thriving semiconductor hub, a number of far-reaching agreements were signed on May 1 to create industry driven R&D programs. The principal projects among these include mass production of "5G Narrowband-IoT- the Koala Chip, Architected and Designed in India"; Development of Advanced Computing for design, manufacture, deployment and maintenance of 10 Lakh Integrated NavIC (Navigation with Indian Constellation) and GPS Receivers; and Partnership for making available Electronic Design Automation (EDA) tools & design solutions for Chips to Start-up (C2S) Programme being implemented at 100+ Institutions for 5 years. These MoU have been signed among industries, academia and relevant government stakeholders.[4]

Recognising the hyper-global nature of semiconductor design, fabrication and the risk to its supply chain, India is also collaborating with its Quad partners under the "Semiconductor Supply Chain Initiative" to strengthen the global semiconductor supply chain's productive capacity and resilience. On May 24, Quad leaders committed to the Common Statement of Principles on Critical Technology Supply Chains[5], to build secure, resilient, diverse and sustainable technology supply chains.[6] This was also echoed at the US-led Indo-Pacific Economic Framework (IPEF) launched in Tokyo on May 23. Speaking as a founder-member of IPEF, the Indian PM highlighted a three-pillar foundation of trust, transparency and timeliness for resilient supply chains.[7]

India's progress and challenges for early rollout of 5G

On May 17, the PM launched India's first 5G Test Bed that will allow start-ups and industry players to test their products, prototypes and algorithms. Till now, this test was only possible abroad. He also set a target for India to roll out 6G services by 2030. 6G will be characterised by provision of advanced services such as truly immersive extended reality (XR), high-fidelity mobile hologram and digital replica.

[4] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1821809

[5] 100347806.pdf (mofa.go.jp)

[6] https://www.mea.gov.in/bilateral-documents.htm?dtl/35357/Quad+Joint+Leaders+Statement

[7] English Translation of Remarks by Prime Minister Shri Narendra Modi at the Announcement of Indo-Pacific Economic Framework (mea.gov.in)

The 5G Test Bed has been developed as a multi-institute collaborative project led by IIT Madras.[8]

The recommendations of the Telecom Regulatory Authority of India (TRAI) regarding the 5G spectrum auction have been generally accepted by the Digital Communication Commission (DCC) of the Department of Telecommunications (DOT), but issues of dissonance remain.

The first one pertains to the 5G spectrum allocation to corporates, in which the DOT has ruled out any direct spectrum allocations to corporates for private 5G networks. The Telecom Regulatory Authority of India (TRAI) had earlier recommended that corporates should be allowed private networks, and arrangements should be made for companies to obtain necessary spectrum on a leasing basis from a licensed entity. [A private network is an extension to a wireless technology for the creation of a dedicated local area network (LAN) within a specific premise or business facility for seamless connectivity needs.]

The second issue of concern between satellite and terrestrial service providers pertains to the mmWave in the 27.5GHz-28.5GHz band. TRAI recommended that since mmWave spectrum will be used for hotspots or micro cells in urban areas to cater to high-capacity requirements, 5G sites can coexist with satellite earth stations. TRAI recommended that DOT should define exclusion zones, by software-defined automated process, for the co-existence of 5G stations and satellite earth stations. However, Satellite players have contended that globally, many countries including the European Union, have kept spectrum for terrestrial and satellite-based services in separate bands. A shared model, as proposed by the TRAI, will harm the business of established and upcoming satellite players.

For Telecom Service Providers (TSP), this band is important for its high-capacity, low-latency, and high-throughput attributes. On May 3, the UK-based Global mobile Suppliers Association (GSA) extended its support to auctioning of all spectrum bands as recommended by the Telecom Regulatory Authority of India, and pointed out that there was "no interference issue" for the satellite services from the 5G systems in this band. The British group further recommended that India's National Frequency Allocation Plan (NFAP) should

[8] India's first 5G testbed set to go live; to support startups to validate products, prototypes, algorithms, Government News, ET Government (indiatimes.com)

be revised to abide by the World Radiocommunication Conference (WRC) 2019 resolutions[9] and frequency bands.[10]

The final decision will be taken by the Union Cabinet on these divergent views.

CERT-In's Directives 2022 present operational challenges

The Computer Emergency Response Team's recently released "Cyber Security Directives 2022" have evoked mixed responses from corporates – especially those related to feasibility of reporting a cyber incident within six hours of detection and maintaining logs of ICT systems for a rolling period of 180 days within the Indian jurisdiction. In a letter dated May 5 to the Indian Computer Emergency Response Team (CERT-In), the Information Technology Industry Council (ITI), the global technology industry lobby, has flagged operational difficulties pertaining to these directives and urged the Indian government to hold fresh stakeholder consultations.[11] Besides flagging the privacy issues pertaining to VPN users, the lobby has also queried the efficacy of synchronizing systems clocks with the Servers of the National Informatics Centre (NIC) or National Physical Laboratory (NPL), contending that companies already have their reliable global sources for time synchronisation and NPL does not have the required infrastructure to disseminate time to a large group of entities.

Responding to industry concerns, the nodal Ministry released FAQs on May 18, which respond to 44 general concerns of industry and would facilitate operationalisation of the Directives.[12]

These FAQs have clarified that the direction regarding Virtual Private Network Service (VPN Service) providers to register and maintain certain specific information about the subscribers/customers, refers to general internet subscribers and do not apply to Enterprise/Corporate VPNs. The logs may be stored outside India also as long as the obligation to produce logs to CERT-In is adhered to by the entities in a reasonable time. It was also clarified that organisations having ICT infrastructures spanning multiple geographies may use accurate and standard time source other than National Physical Laboratory (NPL) and National Informatics Centre (NIC). However, it is to be ensured that their time source shall not deviate from NPL and NIC.[13] On May 20, the Indian

[9] RR-2020-00013-Vol.III-EA5.pdf (itu.int)
[10] spectrum auction: Put entire 28 GHz band up for sale, no interference issue: GSA, Telecom News, ET Telecom (indiatimes.com)
[11] https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
https://www.medianama.com/2022/05/223-iti-letter-cert-cybersecurity-directive/
[12] FAQs_on_CyberSecurityDirections_May2022.pdf (cert-in.org.in)
[13] FAQs_on_CyberSecurityDirections_May2022.pdf-Q 34-42

government has asked virtual private network (VPN) service providers to adhere to the laws of the country, once the directives are operationalised.[14]

AI-powered wargame centre launched

On May 13, the Army Training Command signed a Memorandum of understanding (MoU) with Gandhinagar-based Rashtriya Raksha University (RRU), an institute under the Ministry of Home Affairs (MHA), to develop a 'Wargame Research and Development Centre' in New Delhi. The simulation-based training centre will use artificial intelligence (AI) to design virtual reality wargames that will train the Army to test strategies through "metaverse-enabled gameplay". Apart from the Armed Forces, the Central Armed Police Forces (CAPF) will also be trained in the metaverse-enabled simulation exercises for counter-terror and counter-insurgency operations. The RRU will join hands with Tech Mahindra to develop the centre in next four months.[15]

[14] What is VPN, and how does it work? (indianexpress.com)
[15] RRU to develop wargame centre in Delhi to train soldiers for Indian Army | Cities News, The Indian Express

International Developments

U.S. Offers $15 Million Bounty for Conti Ransomware Gang

The Conti ransomware gang, that had pledged its backing to the Russian government at the start of the Russia-Ukraine War, is being pursued by the US Government. It was reported on May 9 that the US State Department, under its "Transnational Organised Crime Reward Program" (TORCP), is willing to pay up to $10 million for information leading to the identification and/or location of anyone holding a key leadership role in the group. Additionally, the U.S. is offering up to $5 million for information leading to the arrest and/or conviction of any individual in any country conspiring to participate in or attempting to participate in a Conti variant ransomware incident. The initiative hopes to strike a major blow to the Conti ransomware group, that has been responsible for several ransomware incidents over the past two years.[16] A recent "Black Basta" ransomware operation that used malware to encrypt files on compromised systems and has affected a large number of systems, has also been attributed to the Conti Group.[17] On May 19, it was reported that sensing the pursuit, the admin panel of the Conti ransomware gang's official website was shut down.[18]

Israel keen to set up 'Cyber Iron Dome'

On May 2, Israel's National Cyber Directorate ordered communications firms to formulate plans to protect communications networks using a combination of monitoring and control mechanisms to get a real time picture of cyber protection while ensuring privacy. New regulations are currently being implemented in which mandatory and unified standards will have to be met. These efforts are being made to protect Israel's cyberspace and create a kind of 'Cyber Iron Dome', akin to its 'Iron Dome Air-Defence System'.[19]

EU announces its Cyber Posture

On May 23, the Council of the European Union adopted a set of conclusions concerning the development of the EU's Cyber Posture. These conclusions

[16] https://www.securityweek.com/us-offers-15-million-bounty-leaders-conti-ransomware-gang
[17] https://www.securityweek.com/new-black-basta-ransomware-possibly-linked-conti-group
[18] Discontinued: The End of Conti's Brand Marks New Chapter for Cybercrime Landscape (advintel.io)
[19] iron dome: Israel keen to set up cyber 'Iron Dome' to curb rise in attacks, CIO News, ET CIO (indiatimes.com)

stem from the Strategic Compass, the EU's action plan to strengthen its security and defence policy by 2030. The Council emphasises five functions of the EU in the cyber domain: strengthen cyber resilience and capacities to protect; enhance solidary and comprehensive crisis management; promote vision of cyberspace; enhance cooperation with partner countries and international organisations; and finally, prevent, defend against and respond to cyber-attacks. It also emphasises the need to strengthen the fight against international cybercrime, in particular ransomware, through the EMPACT (European Multidisciplinary Platform Against Criminal Threats) mechanism, via exchanges between the cyber security, law enforcement and diplomatic sectors, and through strengthening law enforcement capabilities in investigating and prosecuting cybercrime. The Council commits itself to continuous engagement in relevant international organisations, especially in the UN First and Third Committee-related processes, while emphasising that existing international law applies, in and with regard to cyberspace.

This Cyber Posture will be a step towards establishing an EU doctrine for action in cyberspace, based on enhanced resilience, capabilities and response options, as well as a shared position on the application of international law in cyberspace. The Council will review the progress made on the implementation of these conclusions in 2023.[20]

U.S. Cyber Command conducts 'Hunt forward' operations

The 'Hunt forward' operation is a critical component of the US Cyber Command to protect the US homeland as part of its Cyber Strategy of "persistent engagement," by challenging adversary activities wherever they operate. On May 3, the US Cyber Command Chief, General Paul Nakasone, revealed that in 2021 the Command conducted nine "Hunt Forward" operations in different countries, including Lithuania and Ukraine, where the Cyber Command helped identify and counter vulnerabilities in the foreign affairs and defense ministries' systems. The US Cyber Command has acknowledged twenty-eight "Hunt Forward" operations in the past four years. While the host countries benefit from US cybersecurity tools and threat intelligence, and US Cyber Command gets better visibility into threats beyond its border by putting sensors on these nation's networks.[21]

[20] st09364-en22.pdf (europa.eu)
[21] https://www.cyberscoop.com/nakasone-persistent-engagement-hunt-forward-nine-teams-ukraine/

The US reinforces the Office of National Cyber Director

The US Infrastructure Investment and Jobs Act has set aside a $21 million infusion for the Office of the National Cyber Director (ONCD), and the office is now building out its team. On May 10, the White House announced three new Deputy National Cyber Directors, with Attorney Kemba Walden becoming the inaugural Principal Deputy National Cyber Director. The National Cyber Director serves as a principal advisor to the US President on cybersecurity policy and strategy, and cybersecurity engagement with industry and international stakeholders. The ONCD intends to build out its capabilities and partnerships significantly in Fiscal Year 2022 to support a whole-of-nation effort.[22]

Canada bans China's Huawei and ZTE from its 5G networks

On May 5, the Canadian Industry Minister announced a ban on Huawei and ZTE from its 5G networks. The move is intended to improve Canada's mobile internet services and "protect the safety and security of Canadians". Several nations - including the UK, the US, Australia and New Zealand - have already placed restrictions on the firms. These nations make up an intelligence-sharing arrangement named "Five Eyes", whose network shares classified information. Huawei Canada has termed the decision as purely political, which has nothing to do with cyber security or any of the technologies in question.[23]

While India has not explicitly barred Huawei and ZTE from operating in India, it has mandated compliance to a security framework. Both firms appear to be struggling to meet requirements under India's National Security Directives on Telecommunication Sector (NSDTS) aimed at preserving the integrity of the supply chain. On May 30, it was reported that the two Chinese firms have not yet been given the 'trusted sources' tag, virtually ruling them out of the country's 5G auctions.[24]

South Korea's intelligence agency joins CCDCOE of NATO

On May 5, the National Intelligence Service (NIS) of South Korea became a contributing participant for NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), a cyber defense group based in Tallinn, Estonia. The CCDCOE is a cyber-knowledge hub focused on research, training, and exercises in the field of cybersecurity, established in May 2008. Last month, the

[22] Office of the National Cyber Director | The White House
[23] Canada to ban China's Huawei and ZTE from its 5G networks - BBC News
[24] Huawei: 5G: End of the road for Huawei and ZTE in India?, Telecom News, ET Telecom (indiatimes.com)

NIS had participated in "Locked Shields 2022", a large and complex international live-fire cyber defence exercise, conducted by CCDCOE. Expectedly, China is not happy with South Korea Joining CCDCOE.[25]

[25] South Korea's intelligence agency joins NATO's cyber defense center as first in Asia (koreaherald.com)

International Cooperation

BRICS Ministers reaffirm commitment for secure ICT-environment

The Ministers of Foreign Affairs/International Relations of BRICS countries met virtually on May 19, 2022. In a Joint Statement, the Ministers reaffirmed their commitment to the promotion of an open, secure, stable, accessible and peaceful ICT-environment. They supported the United Nations-led constructive dialogue in promoting ICT-security, including within the UN Open-Ended Working Group (OEWG) on security of and in the use of ICTs 2021-2025, and developing a universal legal framework. They encouraged implementation of the BRICS Roadmap of Practical Cooperation on ensuring security in the use of ICTs.

The Ministers supported information exchanges and technical cooperation on AI technology as declared at the 7th BRICS Communications Ministers meeting. BRICS members have agreed to be guided by the ethical and responsible use of Artificial Intelligence.

The Ministers also expressed concern over the rising complexity of criminal misuse of ICTs and welcomed the ongoing work in the UN Open-Ended Ad Hoc Committee of Experts to draft a comprehensive international convention on countering the use of ICTs for criminal purposes.[26]

Quad Leaders' Joint Statement

Heads of governments of Quad countries met in Tokyo on May 24. Alongside their commitment to a free and open Indo-Pacific, they recognised an urgent need to take a collective approach to enhancing cybersecurity. In a Joint Statement, they laid emphasis on the defence of critical information infrastructures, resilience of supply chains for digitally enabled products and services, and aligning baseline software security standards. They welcomed the initiative for the 'Quad Cybersecurity Day' to enhance protection of users in the Indo-Pacific region.

On Critical and Emerging Technologies, the leaders endorsed the move towards the signature of a new Memorandum of Cooperation on 5G Supplier Diversification and Open RAN, while encouraging Open RAN Track 1.5 events for collaborative efforts with industry. The leaders launched the 'Common Statement of Principles on Critical Technology Supply Chains', that advances cooperation on enhancing resilience against risks to semiconductors and

[26] BRICS Joint Statement on "Strengthen BRICS Solidarity and Cooperation, Respond to New Features and Challenges in International Situation" (mea.gov.in)

other critical technologies. Finally, the leaders encouraged strengthening of cooperation for technology standards through the new "International Standards Cooperation Network (ISCN)".[27]

India-France Bilateral Cooperation

At the India-France summit in Paris on May 4, the leaders welcomed public-private engagement on building standards and protocols for free, inclusive, innovative and open public digital infrastructure. India will participate at "Vivatech", Europe's largest digital fair, in Paris.

Building upon the implementation of the Indo-French roadmap on cyber security and digital technology, both sides reaffirmed their intention to deepen cooperation on Exascale computing technology[28] for developing supercomputers in India. They also agreed to work together for more secure and sovereign 5G/6G telecommunication systems.[29]

***

[27] Quad Joint Leaders' Statement (mea.gov.in)

[28] Exascale computing refers to computing systems capable of calculating at least 10^{18} floating point operations per second. The terminology generally refers to the performance of supercomputer system.

[29] India–France Joint Statement during the Visit of Prime Minister to France (mea.gov.in)

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

www.delhipolicygroup.org