Delhi Policy Group

DPG Cyber Review

Volume 1, Issue 1

FEBRUARY 2020

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

DPG Cyber Review
Volume 1, Issue 1
February 2020

ABOUT US

Founded in 1994, the Delhi Policy Group is among India's oldest independent think tanks with its primary focus on international and strategic issues of critical national interest. Over the past decades, the Delhi Policy Group has established itself in both domestic and international circles, particularly in the area of national security.

In keeping with India's increasing global profile as a leading power and the accompanying dynamism of India's foreign and security policy, the Delhi Policy Group has expanded its focus areas to include India's broader regional and global role; India's initiatives to strengthen its strategic periphery; India's political, security and connectivity challenges and policies across the Indo-Pacific; and the strategic partnerships that advance India's rise. To support these goals, the DPG undertakes research, publishes policy reports and organises conferences on strategic and geo-political, geo-economic, and defence and security issues.

DPG Cyber Review

DPG Cyber Review is compiled by our research team from publicly available information and open source media to provide an overview of significant developments related to cyber and digital technology domains during the month. Your comments and feedback can be addressed to Brig. Abhimanyu Ghosh (Retd.), Senior Fellow at abhi.ghosh@dpg.org.in

Cover Photograph:

US FCC Chairman Ajit Pai interacting with TRAI in New Delhi on February 24, 2020.
Source: Twitter/@TRAI © 2020 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
Volume 1, Issue 1
February 2020

Contents

Abstract

The DPG's Cyber Review is intended to provide insights on the current status of Cyber threats impacting national security, economy and critical infrastructure as well as global stability; technologies that are disrupting the Cyber domain; and measures undertaken by the Government of India to respond to the range of challenges posed by Cyberspace.

The review also highlights International developments in the cyber and digital technology domains that have a bearing on India's national interest.

The information disseminated through this monthly Cyber Review is intended to serve as reference material for all national stakeholders committed to making the Cyberspace a safe, secure, resilient, trusted and vibrant tool for India's development and economic prosperity, while also fostering global cooperation for establishing the rule of law through collaborative actions to curb cross border crime, terrorism and threats to the cyber commons.

National Developments

Cyber Threat Scenario

In India, cyber threats in the last month mostly manifested as attacks in the financial, health and educational sectors by criminals for monetising personal data.

On February 9, 2020, a Singapore-based cyber security company revealed that a database containing more than 450,000 payment card details of Indian banks has been uploaded onto the darknet card shop website Joker's Stash, which is used by cyber criminals to buy and sell card data on the darknet.[1]

In the healthcare sector, an investigation by a German security firm found on February 4, 2020 that nearly one million medical files and 107 million related medical images of Indian patients, including X-rays and scans, are freely accessible on the internet. The records and images include details such as patient name, date of birth and ID, name of the medical institution, ailment, physician names and other sensitive details.[2]

Further, the news media reported on February 17, 2020 that the computer servers of the Indian Institute of Technology, Madras (IIT-M) went down, which was feared to be a cyber-attack that impacted e-mail services.[3]

Digital Technologies

Artificial Intelligence

A National Strategy for Artificial Intelligence (NSAI) discussion paper was released by NITI AYOG in June 2018. It is now reported that an approach paper to create India's cloud computing platform – the AIRAWAT (Artificial Intelligence Research, Analytics and Knowledge Assimilation Platform) has been circulated for comments. AIRAWAT is envisioned to be a leading-edge AI computing technology platform for key players - students, researchers, start-ups, corporates and government organisations.[4]

[1] https://tech.economictimes.indiatimes.com/news/internet/details-of-450000-payment-card-details-of-indian-banks-leaked/74013671 dated February 8, 2020
[2] https://economictimes.indiatimes.com/tech/internet/german-firm-finds-one-million-files-of-indian-patients-leaked/articleshow/73921423.cms dated February 4, 2020
[3] https://www.thehindubusinessline.com/info-tech/cyber-attack-shuts-iit-madras-email-system/article30861902.ece# dated February 19, 2020
[4] NITI AYOG Approach Paper- AIRAWAT: AI Specific Cloud Computing Infrastructure

India's first Artificial Intelligence Summit, RAISE 2020 ('Responsible AI for Social Empowerment 2020') is to be organised by the Government in partnership with industry and academia. The summit scheduled from April 11-12, 2020 in New Delhi, is intended to exchange ideas and chart a course for the use of AI for social empowerment, inclusion and transformation in key areas like Healthcare, Agriculture, Education and Smart Mobility. During the summit, start-ups will be provided the opportunity to showcase their AI solutions aimed at the social transformation, inclusion and empowerment. Interested start-ups around the world can participate in the event. Ahead of the summit, the Ministry of Electronics and Information Technology (MeitY) organised a consultation with industry representatives to build synergies within India's Artificial Intelligence landscape.[5]

5G Technology

The Department of Telecommunications is looking to start 5G field trials in March 2020, having conducted meetings with Telecom Service Providers (TSP) and their gear vendor partners to discuss use-cases and preparedness. Ahead of these trials, DoT has accorded approval to the Chinese telecom and electronics giant Huawei to conduct 5G trials in the country and TSPs have submitted applications for trial with preferred vendors.[6] The DoT will now consult with Wireless Planning and Coordination (WPC) to discuss spectrum allocation.[7]

In its endeavour to identify and promote applications relevant to India in the 5G realm, the DoT launched a '5G Hackathon' on February 21, 2020 in association with NITI Aayog, the Electronics and Information Technology Ministry, Digital India, Start-up India, C-DoT, the Department of Science & Technology, along with academic institutions such as the IITs/IIIT/REC and industry. The Hackathon is aimed at shortlisting India-focussed cutting-edge ideas that can be converted into workable 5G products and solutions. Various phases of the Hackathon include preliminary submission of ideas, selection of 100 best ideas, mentorship and support from the Hackathon partners, development of solutions/products, selection and testing of 30 best solutions/ products on 5G trial network followed by felicitation of the 3 best ideas during

[5] https://www.hindustantimes.com/tech/govt-to-host-artificial-intelligence-focused-raise-2020-summit-in-april/story-MxhpJjYwMK1gQ6co8J7mqJ.html
[6] https://inc42.com/buzz/reliance-jio-airtel-vodafone-ready-for-5g-trials-in-india-after-delay/ dated January 16, 2020
[7] https://telecom.economictimes.indiatimes.com/news/dot-looking-to-start-5g-trials-in-coming-weeks-discusses-use-cases-with-telcos-vendors

India Mobile Congress (IMC), 2020. Stakeholders can participate as individuals or as a team to present use cases for the 5G network in the Indian context.[8]

On February 20, the National Cyber Security Coordinator Lt. Gen. Rajesh Pant stated that India should consider localised manufacturing of telecom equipment by providing a licence fee to China's Huawei Technologies for 5G technology patents. Pant is reported to have stated that "we should give a licence fee to them (Huawei), and ensure that hardware and software would remain ours, and that's the best option," adding that a multi-vendor approach is one of the alternatives to thwart backdoor apprehensions.[9] He further said that the UK, having a source code, has charted a different approach towards Huawei and had established the Huawei Cyber Security Evaluation Centre (HCSEC) way back in 2010. It may be recalled that in January this year, the UK allowed Huawei a limited role in building the country's 5G network, despite intense pressure from the US.

Quantum Technologies

The Government of India, in its budget 2020, has announced a National Mission on Quantum Technologies & Applications (NM-QTA) with a total budget outlay of Rs 8000 Crore ($1.12 billion) in quantum computing research over five years. The next generation transformative technologies that will receive a push under this mission include quantum computers and computing, quantum communication, quantum key distribution, encryption, crypt analysis, quantum devices, quantum sensing, quantum materials, quantum clock and so on. The areas of focus for the Mission will be in fundamental science, translation, technology development, human and infrastructural resource generation, innovation and start-ups to address issues concerning national priorities. Implementation of the mission would help develop and bring quantum computers, secured communications through fibre and free space, quantum encryption and crypt-analysis and associated technologies within reach in the country and help address India specific national and regional issues. Last year, the Department of Science & Technology (DST) had set up a research project named Quantum-Enabled Science & Technology (QuEST) at an institute in Hyderabad, with ₹80 crores ($11.2 million) in funding.[10]

[8] https://pib.gov.in/PressReleasePage.aspx?PRID=1603981 dated February 21, 2020
[9] https://economictimes.indiatimes.com/industry/telecom/telecom-news/india-should-consider-local-manufacturing-of-telecom-equipment-countrys-top-cybersecurity-official/articleshow/74221503.cms dated February 20, 2020
[10] https://thenextweb.com/in/2020/02/01/india-finally-commits-to-quantum-computing-promises-1-12b-investment/

Blockchain

At an event organised on 18 February 2020, Tech Mahindra announced the launch of the T-Block Accelerator, the inaugural accelerator program for the Telangana Blockchain District in partnership with the Government of Telangana and IBC Media, an innovation management company. An MoU had been signed between the Government of Telangana and Tech Mahindra to this effect in 2018. This initiative is aimed at start-ups that have a strong blockchain use-case, thereby accelerating start-up growth and contributing to the growth of the overall industry.[11]

Government Initiatives

Strategy

On February 17, the National Cyber Security Coordinator Lt. Gen. Rajesh Pant said at a public event that the draft of a National Cyber Security Strategy 2020, which envisages creating a secure cyberspace in India, is ready and will soon be sent to key ministries for comments before seeking Cabinet approval. The vision of the strategy is to ensure a safe, secure, resilient, trusted and vibrant cyberspace for India's prosperity.[12]

Organisational Reforms

The Ministry of External Affairs had announced last month the setting up of a New, Emerging and Strategic Technologies (NEST) division. NEST will act as the nodal division within the ministry for issues pertaining to new and emerging technologies, and will facilitate collaboration with foreign partners in the field of 5G and artificial intelligence. The mandate of NEST shall include, but not be limited to, evolving India's external technology policy in coordination with domestic stakeholders and in line with India's developmental priorities and national security goals. Finally, NEST will also help assess foreign policy and international legal implications of new and emerging technologies and technology-based resources and recommend appropriate foreign policy choices.[13]

[11] https://www.expresscomputer.in/blockchain/telangana-govt-and-tech-mahindra-collaborate-to-launch-blockchain-district-accelerator-program/ dated February 19

[12] https://economictimes.indiatimes.com/news/economy/policy/national-cyber-security-strategy-to-go-for-cabinet-nod-soon-rajesh-pant/articleshow/74183503 dated February 18, 2020.

[13] ET Bureau Report of January 2, 2020

On February 25, Minister of State for Home Affairs G. Kishan Reddy inaugurated the National Cyber Research, Innovation and Capacity Building Centre at the Central Detective Training Institute (CDTI) campus at Ramanthapur in Hyderabad. Media reports indicate that the government has anticipated cyber threats and has taken several steps in the recent past such as creating a dedicated division at MHA in October 2017. To further support these initiatives, MHA is also working on setting up Regional Cyber Crime Coordination Centres (R4C) in the States, in collaboration with I4C, to further strengthen the cyber combat capabilities of the nation.[14]

On January 10, Home Minister Shri Amit Shah inaugurated the Indian Cyber Crime Coordination Centre (I4C) and also dedicated the National Cyber Crime Reporting Portal to the Nation. This state-of-the-art Centre is located in New Delhi. The scheme to setup I4C was approved in October 2018 at an estimated cost of Rs.415.86 crore, to deal with all types of cybercrimes in a comprehensive and coordinated manner. It comprises seven components viz., National Cyber Crime Threat Analytics Unit, National Cyber Crime Reporting Portal, National Cyber Crime Training Centre, Cyber Crime Ecosystem Management Unit, National Cyber Crime Research and Innovation Centre, National Cybercrime Forensic Laboratory Ecosystem and Platform for Joint Cyber Crime Investigation Team. At the initiative of Ministry of Home Affairs (MHA), 15 States and UTs have given their consent to set up Regional Cyber Crime Coordination Centres in respective States/UTs.[15]

Budgetary Support

In her Budget 2020 speech to Parliament on February 1, Finance Minister Smt. Nirmala noted that the new economy will be based on innovations that disrupt established business models. Artificial intelligence, Internet-of-Things (IoT), 3D printing, drones, DNA data storage, quantum computing, etc. are re-writing the world economic order.[16]

The Budget proposes to provide ₹6,000 crore to the Bharat Net programme in 2020-21. This outlay will be used to link one lakh gram panchayats this year with Optical Fibre to the Home (FTTH) connections through Bharat Net. This will fulfil the vision of providing digital connectivity to all 'public institutions'

[14] https://www.thehindubusinessline.com/info-tech/union-minister-inaugurates-national-cyber-research-centre/article30905919.ece dated February 24, 2020
[15] https://mha.gov.in/media/whats-new?page=1 and https://pib.gov.in/PressReleasePage.aspx dated January 10, 2020
[16] Posted On: 01 FEB 2020 6:11PM by PIB Delhi

like Anganwadis, health and wellness centres and government schools at the gram panchayat level.

Finance Minister Nirmala Sitharaman has provided an outlay of ₹8,000 crore over a period of five years for the National Mission on Quantum Technologies and Applications to take advantage of Emerging technologies like artificial intelligence (AI), Internet-of-Things (IoT), 3D printing, drones, DNA data storage and quantum computing.

The Finance Ministry is to bring out a policy to incentivise the private sector in building Data Centre Parks throughout the country, thus enabling firms to incorporate data in every step of their value chains.

To encourage Make in India under phased Manufacturing Program (PMP), the Government proposes to increase customs duties on some components for cellular mobile phones from April 1.[17]

Capability Building

The Ministry of Electronics & IT (MeitY) and Data Security Council of India (DSCI) have launched a 'Cyber Security Grand Challenge' with combined prize money of ₹3.2 crore to provide impetus for product innovation in the Cyber Security start-up ecosystem. The nine month long Grand Challenge for Cyber Security is designed to promote a culture of innovation and entrepreneurship by building key cybersecurity capabilities in the country. Under it, participants need to create solutions around six defined 'Problem Statement' areas which include microservices, IoT, Biometrics, Hardware Security, etc. As a unique feature, the IPR of the products being developed as part of the challenge will be owned by the respective start-up and not MeitY or DSCI. During the course of the event, participating teams will be provided with handholding monetary support and mentorship by Cyber Security experts.[18]

It was reported on February 25 that Mobile brand Xiomi will launch Smartphones with new QUALCOMM chipsets (Snapdragon 720G, 662 and 460) that support the Indian version of GPS-Navigation with Indian Constellation (NavIC) developed by Indian Space Research Institute (ISRO).[19]

[17] https://www.indiabudget.gov.in/ dated February 1, 2020
[18] https://meity.gov.in/cyber-security-grand-challenge
[19] https://www.gadgetsnow.com/slideshows/xiaomis-next-smartphone-will-be-the-first-to-have-this-tech-made-by-isro/photolist/74306583.cms

International Developments

Cyber Space

Internationally, Cyber threats during the month emanated from geopolitical adversaries, with attacks directed against government networks, intellectual properties and critical infrastructure.

On February 8, Iran is reported to have repelled a cyberattack that disrupted the country's internet services for an hour by employing Dejfa Shield, Iran's so-called digital fortress against cyber-attacks[20].

A ransomware infection at a natural gas compression facility in the United States resulted in a two-day operational shutdown of an entire pipeline asset, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) announced on February 18. According to CISA, the cyberattack affected control and communication assets on the target's operational technology (OT) network.[21]

On February 10, the US Department of Justice announced that a US federal grand jury in Atlanta had returned an indictment charging four members of the Chinese People's Liberation Army (PLA) with hacking into the computer systems of the credit reporting agency Equifax and stealing personal data of US nationals and Equifax's valuable trade secrets. The nine-count indictment alleges that these personnel were members of the PLA's 54th Research Institute, a component of the Chinese military, who conspired with each other to hack into Equifax's computer networks, maintain unauthorized access to those computers and steal sensitive, personally identifiable information of approximately 145 million Americans.[22]

On February 20, **Britain and the United States accused Russia of orchestrating a "reckless" cyber assault on Georgia last year as part of an aggressive campaign of online attacks worldwide.**[23]

Meanwhile, a US Court ruled on February 18 that Washington has the right to block US federal agencies from buying products by Huawei on cybersecurity

[20] https://financialtribune.com/articles/sci-tech/102062/iran-repels-cyberattack-targeting-internet-backbone dated February 08, 2020
[21] https://www.securityweek.com/operations-us-natural-gas-facilities-disrupted-ransomware-attack
[22] https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking dated February 10, 2020.
[23] https://www.securityweek.com/us-uk-blame-russia-2019-cyber-attacks-georgia

grounds, dismissing the Chinese telecom giant's legal challenge to a purchase ban. Huawei had filed the suit nearly a year ago, claiming that Congress had failed to provide evidence to support a law that stopped government agencies from buying its equipment, services, or working with third parties that are Huawei customers. Concerns have intensified in the US with Huawei's rise to become a world leader in telecom networking equipment and one of the top smartphone manufacturers alongside Samsung and Apple. However, the firm is still expected to play a major role in the rollout of ultra-fast 5G networks that will allow wide adoption of next-generation technologies such as artificial intelligence.[24]

Digital Technologies

5G Technologies

The emerging networking techniques such as Software Defined Network (SDN) and Network Function Virtualization (NFV) are promising a complete paradigm shift in how future networks are managed. With their enormous benefits which include reducing the operational cost, better resource utilisation and easier management requirements, the adoption of such technologies is gaining momentum. However, the integration of SDN and NFV with current systems faces many challenges that will require deep analysis to propose creative solutions.

The Fourth International Workshop on Software Defined Network and Network Function Virtualization (SDN-NFV 2020) is scheduled to be held in Paris April 20-23, 2020. The workshop is aiming to invite researchers from both academia and industry to present their state-of-the-art research results, ideas, developments, and applications in the areas of SDN, NFV, 5G, Internet of Things (IoT) and Edge Computing. The deadline for submission of Research papers was February 01, 2020.[25],[26]

The White House is reportedly working with U.S. technology companies to create advanced software for next-generation 5G telecommunications networks. The plan would build on efforts by some U.S. telecom and technology companies to agree on common engineering standards that would allow 5G software developers to run code. Further, President Trump's top economic adviser said on February 21 that the United States will host a

[24] https://www.thehindubusinessline.com/info-tech/huawei-loses-legal-challenge-of-us-federal-purchase-ban/article30858706.ece dated February 19 2020
[25] http://www.guide2research.com/conference/sdn-nfv-2020
[26] http://emergingtechnet.org/SDN-NFV2020/

conference with Huawei rivals to try and accelerate development of affordable competing 5G wireless technology.[27]

Japan is reportedly planning a comprehensive strategy for "post-5G" (6G) technology by 2030 and it is believed that the new technology will be 10-times faster than the current 5G. The Ministry of Internal Affairs and Communications of Japan set up a government-civilian research society in January this year under the chairmanship of the University of Tokyo Goshinjin, and under the direct supervision of the General Affairs Minister. Additionally, people from NTT and Toshiba will also be invited to discuss 6G performance goals and policy support by June this year.[28]

With the acceleration of 5G commercialization and 6G research picking up across the globe, various mobile operators and service providers are moving towards disaggregated and open reference architecture that utilizes open components with standard APIs from a multi-vendor ecosystem. Open Radio Access Network (O-RAN) also aims at automating mobile networks and build intelligent SDN. It also makes networks programmable and autonomous to cope up with the growth in ML, AI, automation and low latency applications. By leveraging Software Defined Network (SDN) and Network Function Virtualization (NFV), mobile operators and service providers have successfully designed competitive and open core networks. The first edition of the Next Generation Radio Access Networks (RAN) Workshop will be held in conjunction with IEEE Wireless Communications and Networking Conference (WCNC) in Seoul on April 6-9, 2020 on the theme 'OPEN-RAN: Open Road to Next Generation Mobile Networks'. Participants were requested to submit Camera ready Papers by February 15, 2020.[29]

IoT Devices

On 20 February 2020, IANS reported that new research suggests that a new ultra-low power Wi-Fi radio housed in a chip smaller than a grain of rice can pave the way for battery-less smart devices and more portable, fully wireless smart home setups. The device, developed by electrical engineers at the University of California San Diego in the US, enables Internet of Things (IoT) devices to communicate with existing Wi-Fi networks using 5,000 times less power than today's Wi-Fi radios. Commercial Wi-Fi radios typically consume hundreds of milliwatts to connect IoT devices with Wi-Fi transceivers. As a

[27] https://in.reuters.com/article/us-telecoms-5g-kudlow/u-s-will-host-5g-conference-including-companies-in-about-a-month-kudlow-idINKBN20F1ZX dated February 21, 2020.
[28] https://www.expresscomputer.in/internet/move-over-5g-japan-to-launch-6g-by-2030/45676/
[29] https://wcnc2020.ieee-wcnc.org/workshop/ws-01-open-ran

result, Wi-Fi compatible devices need either large batteries, frequent recharging or other external power sources to run.

The International Solid-State Circuits Conference ISSCC 2020 conference was held in San Francisco on February 16-20, 2020.[30]

[30] https://www.expresscomputer.in/news/new-chip-may-pave-way-for-batteryless-smart-devices

India-US Bilateral Cooperation

The President of the United States visited India on February 24-25, 2020. The Joint Statement on Vision and Principles for India-U.S. Comprehensive Global Strategic Partnership, issued at the conclusion of the Modi-Trump Summit, included the following paragraph on bilateral cooperation in cyberspace and digital technologies:

> *"India and the United States are committed to an open, reliable, and secure Internet that facilitates trade and communication. India and the United States recognized the need for an innovative digital ecosystem that is secure and reliable, and facilitates the flow of information and data. The leaders intend to foster cooperation among their industry and academia for open, secure, and resilient supply of strategic materials and critical infrastructure, and to independently evaluate the risk associated with deployment of emerging technologies."*[31]

Further, on the sidelines of the Modi-Trump Meeting, The US Federal Communications Commission (FCC) Chairman Mr Ajit Pai met Telecom Secretary Anshu Prakash on February 24, 2020, and discussed issues ranging from spectrum to 5G. Subjects covered in their discussions included 5G, tele density, optical fibre, spectrum bands and their auction process. The two sides reportedly resolved to work more closely on measures to improve spectrum efficiency. The FCC Chairman was also informed about Low Mobility Large Cell (LMLC) plans which India has developed for rollout of 5G technology in rural areas. Separately, Mr. Ajit Pai also met the Chairman of Telecom Regulatory Authority of India (TRAI) on February 24, 2020.[32]

[31] https://mea.gov.in/bilateral-documents.htm?dtl/32421/Joint+Statement+Vision+and+Principles+for+IndiaUS+Comprehensive+Global+Strategic+Partnership

[32] PTI | February 24, 2020, 21:03 IST

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

www.delhipolicygroup.org