Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

AUGUST 2021

Volume II, Issue 8 | August 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 8
August 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 8
August 2021

Contents

Abstract

The past month has witnessed criminal attacks on Indian cyberspace targeting schools, universities, research centres and financial portals. Pakistan state agencies are reported to be targeting Indian cyberspace with mutated malware. To meet these challenges, the National Security Council Secretariat (NSCS) and the Ministry of Home Affairs have taken measures to enhance India's cybersecurity posture and prevent cyberattacks.

The government has announced liberalised 'Drone Rules 2021,' adopting a proactive regulatory approach to make India a global drone hub by 2030. The country's first 'Quantum Computer Simulator (QSim) Toolkit', a collaborative effort of academia and industry and funded by the government, was launched this month to develop skills of quantum computing linked technologies. A similar collaborative effort is being seen in the semiconductor sector for developing memory technology.

On the international front, ransomware attacks continue to dominate cyberspace. Safeguarding customer information has become a challenge for telecom service providers. Data on some 47 million customers of the US telecommunications company T-Mobile was reportedly stolen. In Japan, the crypto currency exchange Liquid has been targeted, resulting in a loss of $97 million in various crypto-currencies.

To meet continuing cyber threats across sectors, the US plans to allocate $2 billion from the $1.2 trillion infrastructure bill to improve cybersecurity capabilities. US private sector technology companies have also pledged large investments, as part of joint initiatives to boost the nation's cyber security. Meanwhile, China continues to expand strict regulatory measures on digital companies, including through a Personal Information Protection Law and a Data Security Law which be effective from November 1 and September 1 respectively.

The National Security Advisers of the BRICS and IBSA countries held separate meetings during the month to review emerging threats to national security and strengthen cooperation on cyber security.

National Developments

Cyber Threat Scenario in India

There have been continuous attempts to launch cyber-attacks on Indian cyberspace. The Indian Computer Emergency Response Team (CERT-In) observed over 6.07 lakh cyber security incidents in the first six months of 2021, of which about 12,000 incidents were related to government organisations.[1]

Indian schools, universities and research centres have been targets of cyberattacks due to their lack of resources. According to a Check Point Research (CPR) report released on August 18, the education sector in India experienced 5,196 attacks per week on average during the month of July. The most targeted countries were India, Italy, Israel, Australia and Turkey.[2] Another report of August 11 indicated that multiple financial institutions using software from digital payment services provider Pine Labs were attacked by the ransomware 'DeepMatter'. The Cyble Research Lab, investigating this breach, found that personal records of over 500,000 individuals were affected.[3]

Pakistan adopts mutated malware to target India

Pakistan-originated malware that had earlier targeted the power sector and government organisations in India has now mutated, like a real-life virus, to adopt new cyber-attack capabilities.[4] The modified remote access trojan, dubbed as 'ReverseRat 2.0', has added functionality such as taking remote photos via webcams and retrieving files on USB devices inserted into the compromised machines. The mutated version included new evasion techniques to counter Kaspersky or Quick Heal antivirus (AV) products deployed in India. A report by Black Lotus Labs posted On August 11 suggested that Afghanistan, India, Iran and Jordan were among those targeted by attackers using a forged United Nations Meeting platform (UNODC) to lure the government targets.[5]

[1] More than 6.07 lakh cyber security incidents observed till June 2021: Government - The Hindu
[2] https://www.thehindu.com/sci-tech/technology/internet/indias-education-sector-witnessed-most-number-of-cyberattacks-in-july/article35996641.ece
[3] https://blog.cyble.com/2021/08/11/blackmatter-ransomware-attack-impacting-multiple-financial-institutions/
[4] Pakistan's cyber-attack malware mutates, adopts nefarious new capabilities - India News (indiatoday.in)
[5] https://blog.lumen.com/reverserat-reemerges-with-a-nightfury-new-campaign-and-new-developments-same-familiar-side-actor/

Capability building measures to meet Cyber threats

On August 4, the government announced in Parliament that it has taken a number of steps to enhance India's cybersecurity posture and prevent cyberattacks, including formulation of a Cyber Crisis Management Plan.[6]

On August 10, the National Security Council Secretariat (NSCS) issued 'mandatorily applicable' guidelines to check cyberattacks on critical information infrastructure. These guidelines provided a "baseline requirement" for cybersecurity audits to check cyberattacks on critical infrastructure which can impact national security, public health and safety, economy and critical operations of the government. The new NSCS guidelines cover six aspects: management, protection, detection, response, recovery and lessons learnt.[7]

Cyber audit is an important facet of information assurance. On August 16, Indian Computer Emergency Response Team (CERT-In) empaneled Siemens for providing information security auditing services to government organisations.[8]

To provide enhanced training to law enforcement personnel,18 states have established state-of-the-art cyber forensic-cum-training laboratories, besides the National Cyber Forensic Laboratory (NCFL) operationalised at MHA, as part of the "Indian Cyber Crime Coordination Centre (I4C)". Using these facilities, more than 28,000 police and law enforcement personnel and about 1,000 judicial officers have been trained so far.[9]

Liberalised Drone Rules 2021

Unmanned Aircraft Systems (UAS), commonly known as drones, offer tremendous benefits to virtually all sectors of the economy, including emergency response, transportation, geo-spatial mapping, defence and law enforcement. In view of its traditional strengths in innovation and information technology, as well as huge domestic demand, India has the potential to be global drone hub by 2030. To spur growth of India's nascent drone industry, on

[6] https://www.deccanherald.com/national/12001-cybersecurity-incidents-related-to-govt-organisations-observed-in-h1-2021-govt-1016177.html
[7] NSCS issues 'mandatorily applicable' guidelines to check cyberattacks on critical infra, Government News, ET Government (indiatimes.com)
[8] https://www.crn.in/news/cert-in-empanels-siemens-to-provide-information-security-audit-service/
[9] https://ciso.economictimes.indiatimes.com/news/digital-crime-on-rise-mha-helps-18-states-to-get-cyber-forensic-labs/85202469

August 26 the government announced liberalised 'Drone Rules 2021,' superseding the UAS Rules 2021 of March this year.[10]

There are 30 key features of these Rules, which are oriented around trust, self-certification and non-intrusive monitoring. Classification of drones are based on their maximum weight. No remote pilot licence is required for micro drones (for non-commercial use) and nano drones. Mandatory safety and security features include 'No permission-No take off' hardware, real time tracking beacon, unique identification number and geofencing capability. A multi-stakeholder drone promotion council will be set up to facilitate a growth-oriented regulatory regime.

The most important change in these Drone Rules 2021 is the launch of an interactive airspace map with green, yellow and red zones, which will be notified within 30 days, on the country's single-window drone platform 'Digital Sky'. No permission is required for operating drones in green zones. Drone corridors will be developed for cargo deliveries.[11]

As part of capability building for the drone ecosystem, on August 12 the company MapmyIndia announced a partnership with the Drone Federation of India to launch and fund a 'Drone Innovation Challenge'. Software development to create significant value addition for the drone ecosystem will be part of this challenge.[12]

The Indian company DCM Shriram is investing in a Turkish drone maker to create a global UAV company for various applications in civilian and military fields. On August 18, DCM Shriram signed a partnership deal with Turkey's Zyrone Dynamics on the side lines of the International Defense Industries Fair (IDEF) in Istanbul. DCM Shriram is investing $1 million in Zyrone Dynamics, taking a 30 per cent stake in the company.[13]

Along with these welcome initiatives to make India a drone hub, there is also a need to develop a robust counter-drone strategy.

India's first Quantum Computer Simulator toolkit launched

Quantum computing promises exponential growth in several areas, including cryptography and machine learning. On August 28, the Ministry of Electronics

[10] https://pib.gov.in/PressReleasePage.aspx?PRID=1749154
[11] https://pib.gov.in/PressReleasePage.aspx?PRID=1749154
[12] https://www.outlookindia.com/newsscroll/mapmyindia-partners-drone-federation-of-india-for-drone-innovation-challenge/2139984
[13] India's DCM Shriram buys 30% stake in Turkish drone maker - The Week

and Information Technology (MeitY) launched the country's first 'Quantum Computer Simulator (QSim) Toolkit'. QSim has been jointly developed by the Indian Institute of Science (IISc), Centre for Development of Advanced Computing (CDAC) and IIT Roorkee, based on IBM's open-source framework. The toolkit provides a platform for students to acquire the skills of 'programming' and 'designing' real Quantum Hardware in a cost-effective manner.[14] The government had allocated ₹8,000 crore ($ 1091 million) in the annual budget of 2020 for developing quantum computing linked technologies under the National Mission on Quantum Technologies and Applications.

Initiatives for Semiconductor design and production

Memory technology is critical for semiconductors to enhance data security and design of 'perfect' chips. On August 18, the Department of Space's Semi-Conductor Laboratory (SCL), Mohali, and the Indian Institute of Technology, Bombay (IITB) announced a partnership to establish CMOS 180nm-based production-ready 8-bit secure memory and encryption technology. In contrast to the high voltage required by earlier one-time programmable memory (OTP), IITB's memory chip requires less power and chip-area.[15]

Development of standards, product design and semiconductor manufacturing are important for 'Atmanirbhar Bharat'. The challenge, however, remains to translate such technologies from research to manufacture and to establish a vibrant semiconductor ecosystem. Semiconductor manufacturing requires high investments and expertise, which are presently lacking in India. In a welcome development, on August 3 major industry group Tata announced its intention to enter the semiconductor segment, amidst significant shortage of semiconductors worldwide which is impacting various industries.[16]

Pegasus tool controversy

Hearings on the Pegasus tool controversy are continuing at the Indian Supreme Court. On August 17, the government representative contended that it was not in public interest to divulge information on the issue, as national security aspects are involved. It was suggested that a committee of technical experts be constituted to examine all aspects of the issue. The Supreme Court,

[14] https://indianexpress-com.cdn.ampproject.org/c/s/indianexpress.com/article/education/indias-first-quantum-computer-simulator-qsim-toolkit-launched-a-collaborative-initiative-of-iit-roorkee-iisc-bangalore-and-c-dac-7475085/lite/

[15] DST and IIT Bombay jointly develop tiny memory to make chips 'perfect', Government News, ET Government (indiatimes.com)

[16] Post 5G equipment, Tata Group looks to enter semiconductor manufacturing - BusinessToday (ampproject.org)

while issuing a notice to the union government to file its response to pleas seeking an independent probe into the alleged use of the Pegasus surveillance tool, made it clear that it did not want the government to disclose anything which might compromise national security.[17]

[17] Pegasus row: SC issues notice to Centre, says govt need not disclose anything which compromises national security - The Economic Times (indiatimes.com)

International Developments

Ransomware attacks dominate Global Cyberspace

Ransomware attacks surged globally in the first half of 2021, with 304.7 million reported incidents. It is estimated that these attacks grew by 64% between August 2020 and July 2021 across key verticals, including government, education, healthcare and IT industry. On August 11, Accenture, a Fortune 500 IT Consulting Firm, publicly confirmed that some of its systems were infected with 'LockBit' Ransomware. It was reported that hackers have demanded a ransom of $50 million in exchange for 6TB of data. Earlier, ransomware operator REvil had demanded $70 million to decrypt victim files of IT management software firm Kaseya. The global Ransomware loss in 2021 is projected to reach $ 20 billion and it is predicted that by 2031, these attacks will cost around $ 265 billion annually.[18]

To meet ransomware threats, the US Cybersecurity and Infrastructure Security Agency (CISA) is collaborating with several technology companies to operationalise a Joint Cyber Defence Centre. The centre will be involved in coordinating national cyber defence, sharing threat intelligence, and participating in joint exercises.[19]

New child safety feature by Apple raises controversy

On August 5, Apple announced a new feature to limit the spread of sexually explicit images involving children. The machine learning (ML)-based tool will be deployed in the iMessage app to scan photos and determine whether they are sexually explicit, to warn children and their parents.[20] In the US, child pornographic content is tagged as Child Sexual Abuse Material (CSAM) and reported to the National Centre for Missing and Exploited Children (NCMEC), which works with law enforcement agencies. Several experts and advocacy groups have raised concerns that the new feature could potentially become a backdoor channel for government surveillance. However, Apple's senior executives have contended that user privacy will be protected while deploying the technology tool which is intended to root out illegal child pornography.[21]

[18] Accenture knew about ransomware attack in late July: report - Security - CRN Australia
[19] https://www.the420.in/fight-against-ransomware-tech-giants-amazon-microsoft-google-join-us-cyber-team/
[20] Apple's child safety feature explained - The Hindu
[21] https://www.wsj.com/articles/apple-executive-defends-tools-to-fight-child-porn-acknowledges-privacy-backlash-11628859600?mod=followjoannastern

Surveillance Camera Videos hacked Inside Iran's Prison

On August 24, it was reported that a hacktivist group calling itself Adalat Ali (Justice of Ali) had reportedly broken into computer systems belonging to Iran's Evin prison, where Iranian and foreign political detainees are housed. Several hundreds of gigabytes of documents and images were stolen, including videos taken from the prison's CCTV cameras. The videos and still images purportedly leaked from the prison have 2020 and 2021 timestamps and were sent to several media outlets. Evin prison is on the US and European sanctions list since 2018. The leaks came weeks after a cyberattack struck Iran's national railway system, causing delays and cancellations of hundreds of trains.[22]

T-mobile data breach impacts millions of customers

US telecommunications provider T- Mobile, with more than 100 million subscribers, reported on August 16 that it had suffered an intrusion into its database and was investigating the extent of the breach, after personal data on some of its wireless subscribers was found for sale on the dark web. The information, sold for roughly $280,000 in bitcoin, reportedly included names, dates of birth, phone numbers, addresses, social security numbers, and driver's license information of nearly 47.8 million T- Mobile customers. A 21-year-old hacker claimed responsibility for the attack. T-Mobile has signed long-term partnerships with security companies to provide scalable security solutions that are more resilient to future cyber threats. Safeguarding customer information has been a frequent challenge for U.S. telecom service providers.[23]

Japanese Cryptocurrency Exchange hit by Cyber attack

On August 19, Japanese cryptocurrency exchange Liquid announced that it was victim to an attack that resulted in large amounts of crypto-currency assets being stolen. Hackers were able to compromise its warm wallets, resulting in a loss of $97 million in various crypto-currencies.[24] Warm wallets are usually online and are used for easily accessing and trading funds. Cold wallets, on the other hand, are stored offline and are considered more secure. The company is currently investigating and, in the meantime, has suspended deposits and withdrawals.[25]

[22] https://zetter.substack.com/p/hackers-leak-surveillance-camera
[23] T-Mobile Says Hackers Breached Company Database - WSJ
[24] https://www.cnbc.com/2021/08/19/liquid-cryptocurrency-exchange-hack.html
[25] https://www.securityweek.com/hackers-steal-97-million-japanese-crypto-exchange-liquid

US infrastructure bill allocates $2-billion for cybersecurity

On August 24, the US House passed a measure approving a $3.5 trillion budget blueprint and committing to take up a $1.2 trillion bipartisan infrastructure bill by September 27. The infrastructure bill, which was finalised by the Senate on August 5, includes roughly $2 billion for improving cybersecurity capabilities by developing solutions to identify and mitigate vulnerabilities, improve the security of field devices and addressing issues related to workforce and supply chains. A total of $550 million has been allocated to enhance the security of the power grid. It also includes the Cyber Response and Recovery Fund, which provides $20 million per year until 2028 for assisting government and private sector organisations responding to cyber incidents.[26]

Further, the bill includes $42.5 billion in grants to states to subsidise companies, local governments, or nonprofits to build high-speed broadband internet infrastructure in regions where such technology does not currently exist.[27]

Tech companies pledge billions to boost US cybersecurity

Business leaders from key technology and insurance sectors pledged to partner with the government to boost cyber security efforts in the US, following a meeting with President Joe Biden on August 25, where he described cybersecurity as a "core national security challenge". The meeting was held amidst a wave of ransomware and other cyberattacks that have escalated tensions with US adversaries and had prompted Biden to issue an executive order in May. It was recognised at the meeting that nation-state actors, cybercriminals and other malicious actors continue to target weaknesses in software supply chains and legacy institutions and vendors who lack tools or expertise to stop them. Several initiatives were announced by the White House at the end of the meeting. These include collaboration between the National Institute of Standards and Technology (NIST) with industry and other partners to develop a new framework to improve the security and integrity of the technology supply chain. The Biden Administration also announced the formal expansion of the Industrial Control Systems Cybersecurity Initiative to include electric utilities and natural gas pipelines.

Responding to Biden's call to the private sector to raise the bar on cybersecurity, several US companies pledged large investments. Microsoft will invest $20 billion over the next 5 years to accelerate efforts to integrate cyber security by design. It also announced $150 million in technical services to help federal,

[26] https://www.securityweek.com/us-infrastructure-bill-allocates-2-billion-cybersecurity
[27] U.S. Government Wants a Greater Role in How Americans Access Internet - WSJ

state, and local governments with upgrading security protection training. Google pledged $10 billion over the next five years to expand zero-trust programs and help secure the software supply chain. The company has also pledged to train 100,000 Americans in data analytics, data privacy and security. IBM announced it will train 150,000 people in cybersecurity skills over the next three years, while Amazon planned to offer a multi-factor authentication device to all Amazon Web Services (AWS) account holders for free. Apple will work with its suppliers to drive the mass adoption of multi-factor authentication, security training, vulnerability remediation, event logging, and incident response.[28]

China sponsors private hackers

While the US is struggling to secure its cyber space, China's intelligence agencies are increasingly recruiting from a vast pool of private-sector talent. It was reported by the New York Times on August 27 that this new breed of hackers target government and private institutions alike, mixing traditional espionage with outright fraud and other crimes for profit. Under this system, Chinese hackers have become increasingly aggressive. Investigators believe that these groups have been responsible for recent high profile data breaches, including the Microsoft email system used by many of the world's largest companies and governments. The shift in Chinese tactics was noticed after the responsibility of cyber espionage was reportedly transferred to the Ministry of State Security (MSS) from the People's Liberation Army (PLA) following a slew of sloppy attacks and a reorganisation of the military.[29]

China Passes Data-Privacy Laws

On August 20, China's legislature passed a Personal Information Protection Law (PIPL), placing legal restrictions on how personal data can be collected, processed and protected after it comes into effect on November 1. It calls on any organisation or individual handling Chinese citizens' personal data to minimise data collection and to obtain prior consent. Violating the new privacy law could result in a fine of up to $7.7 million, or up to 5% of the preceding year's business income. The law also calls for handlers of personal information to designate an individual in charge of personal information protection, and calls for handlers to conduct periodic audits to ensure compliance with the law.

The Personal Information Protection Law, along with the Data Security Law, are set to govern China's internet in the future. The Data Security law, to be

[28] FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity | The White House
[29] https://www.nytimes.com/2021/08/26/technology/china-hackers.html?smid=em-share

implemented from September 1, mandates companies to obtain approval from law enforcement agencies to transfer data stored in China to overseas entities. The Personal Information Protection Law, meanwhile, closely resembles Europe's General Data Protection Regulation, known for its robust privacy frameworks. The rules add to Beijing's tightening of regulations, particularly centred around data, which impact the way China's technology giants operate. Following the notification of these laws, the stocks of Chinese big tech companies have suffered a major slump, prompting concerns among investors.[30]

[30] https://www.wsj.com/articles/china-passes-one-of-the-worlds-strictest-data-privacy-laws-11629429138?mod=tech_lead_pos3

International Cooperation

BRICS and IBSA discuss Cyber Security

On August 24, the national security advisers of the BRICS countries reviewed the regional and global geopolitical scenario and emerging threats to national security, including cyber security. The NSAs agreed to strengthen cooperation in cyber security by sharing information, exchanging best practices, capacity building and combating cyber-crimes.[31] India also hosted the inaugural meeting of the National Security Advisers of the India-Brazil-South Africa Trilateral Cooperative Forum (IBSA) grouping on August 25. Representatives from the three countries agreed to expand practical cooperation in cyber security and accepted India's offer to host a meeting of the Cyber Security Experts Group. They also agreed to strengthen coordination on cyber and ICT issues at the UN. [32]

[31] Meeting of the BRICS High Representatives Responsible for National Security (mea.gov.in)
[32] Inaugural Meeting of the IBSA National Security Advisers (mea.gov.in)

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

www.delhipolicygroup.org