Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

DECEMBER 2021

Volume II, Issue 12 | December 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 12
December 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 12
December 2021

Contents

Abstract

2021 saw cyberattacks increasing in scale and sophistication. Criminals with links to states were undeterred by several measures taken at the global and national levels. It appeared that the digital space is competing with the public health sector in churning out different variants of viruses that are impacting national economy and security. India was the sixth largest victim of ransomware attacks, with around 12.1 lakh cybersecurity incidents were observed till October 2021.

Pakistani and Chinese agencies continue to attack the Indian Cyber and Information space. The Indian government banned two news websites and 20 YouTube channels linked to Pakistan's disinformation network for fake content affecting public order. Among rising threats and growing sophistication of attacks by adversaries, the government announced the setting up of a Unified Task Force, synergising the efforts of security and cyber agencies. It also mandated retention of call data and internet usage records for two years to facilitate the work of law enforcement authorities. For better border management along the LAC in Ladakh, telecom infrastructure is being upgraded.

5G trials are being effectively carried out by telecom service providers and equipment vendors across cities and villages with the allotted trial frequency spectrum. To test Indian use cases and technologies, test beds have been created. The indigenous 5Gi standard has been merged with global 3GPP-5G standards, paving the way for global deployment with high-speed, high-quality and inter-operable connectivity. However, challenges remain in terms of spectrum rationalisation and infrastructure.

To boost the semiconductor and display manufacturing eco-system in India, the government has announced a $10 billion scheme under the India Semiconductor Mission that will provide up to 50% incentives to chip manufacturers. Further, to retain chip design patents and IPR in India, it has launched 'Chip to Start-up' program under the 'Design linked incentive' scheme. Several global and Indian companies have shown interest.

In spite of sanctions and high level meetings to curb cyberattacks, ransomware gangs across the globe remain undeterred. Millions of dollars are being extorted by encryption and the promise of decryption of data in exchange for ransom. Meta has banned several Facebook and Instagram accounts of 'surveillance for hire' firms.

Australia announced plans for a licensing framework for cryptocurrency exchanges and launching of a retail central bank digital currency (CBDC). The UK government launched one of the world's first national standard for algorithmic transparency to support significant decisions affecting individuals. It also launched its National Cyber Strategy 2022 to guide its activities in cyberspace to protect and promote national goals.

National Developments

Indian Cyber Threat Scenario

The shift to remote and hybrid work during the Covid-19 pandemic has expanded the "attack surface" and made Indian companies easier targets for ransomware attacks. On December 8, it was reported that 49% of organisations in India suffered multiple ransomware attacks, while 76% were hit by at least one ransomware attack in the past 12 months. The report found that India accounted for the highest average extortion fee payment ($ 1.128 million), while 26% of Indian companies had paid ransoms ranging from $5 million to $10 million.[1]

Parliament was informed on December 10 that more than 700 cases were registered in 2020 for violation of privacy under Section 66E of the Information Technology Act, 2000.[2] India has also seen an alarming rise in cyberattacks against both critical installations and important personalities.

The Indian PM's personal Twitter account was hacked for a brief period on December 12, posting a fake tweet that India has "officially adopted bitcoin as legal tender" with a link promising bitcoin distribution. The hack came after the Indian government's move to introduce in parliament the "Cryptocurrency and Regulation of Official Digital Currency Bill, 2021" which seeks to prohibit private cryptocurrencies in India with some exceptions, and to create an official digital currency to be issued by the Reserve Bank of India. CERT-IN ordered a high-level inquiry into the incident, while Twitter confirmed having taken necessary steps to secure the compromised account.[3]

There were also attacks on India's information space. On December 21, the Union government banned two news websites and 20 YouTube channels for featuring "anti-India content" by invoking emergency provisions of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.The content ranged from "blasphemous" to materials that "blatantly impinge on India's security and sovereignty", and was orchestrated by Pakistan based coordinated disinformation networks.[4] YouTube confirmed compliance with the order to block the channels.

[1] India tops the list in ransomware attacks amid digital push (livemint.com)
[2] Over 740 cases registered under IT Act in 2020 for privacy violation, IT Security News, ET CISO (indiatimes.com)
[3] Crypto scam link posted from Modi's Twitter account as hackers target PMO- The New Indian Express
[4] 20 YouTube Channels 2 Websites Banned In India

Pakistani hacker groups are also targeting Indian government officials. On December 6, a Pakistan based hacker gang "Side copy" was identified for targeting Indian and Afghan officials to steal sensitive Google, Twitter and Facebook credentials. The APT group attempts to mimic the infection chains associated with the SideWinder supply chain attack to mislead attribution. Targets included the Administration Office of the President (AOP) and Ministry of Finance of Afghanistan, and educational services in India. Facebook owner Meta has taken steps to block malicious activities carried out by the group on its platform.[5]

Unified cyber security task force by March

Cyberattacks incorporating ransomware, social engineering and supply chain exploitation and covering the entire spectrum, from espionage to crime and critical infrastructures, which are sponsored by nation states, are getting more sophisticated. The need for a coordinated response is well recognised. On December 20, the government announced the setting up of a specialised unified task force, synergising the efforts of security and cyber agencies including CERT-IN and NCIIPC, with inputs from like-minded friendly countries. The Unified Task Force would also include a Telecom Cybersecurity sub-Task Force to focus on the vulnerabilities posed by the telecom industry. The government is also finalising a "trusted sources" list for procuring telecom gear for 5G and has taken the initiative to address privacy and security issues in mobile phones.[6]

Data retention time extended to investigate cyber crimes

On December 21, the Department of Telecom (DoT) amended telecom licensing conditions stipulating extended duration of archiving call data and internet usage records to two years from one year for security reasons. The amendment mandates telecom companies to maintain internet data records of subscribers, including login and logout details of all subscribers for services provided such as internet access, e-mail, internet telephony services like calls made from mobile applications or Wi-Fi calling, for at least two years.[7] The amendment was extended to other forms of telecom permits on December 22.

[5] cybersecurity: Pakistani hackers targeting Indian, Afghan government, military officials: Report, IT Security News, ET CISO (indiatimes.com)
[6] Unified cyber security task force by March: Source - Times of India (indiatimes.com)
[7] call data record: Govt mandates telcos to keep call data, internet usage record for minimum 2 years, Telecom News, ET Telecom (indiatimes.com)

Boosting telecom infrastructure in Ladakh

India and China share 3,488 km of a shared border, out of which 1,597 km is in Ladakh. Due to better telecom infrastructure and roads on their side, the Chinese PLA find it easier to patrol along the LAC. Indian border troops are disadvantaged by inadequate telecom connectivity to share information with locals. This is soon going to change.

On December 15, it was reported that telecom infrastructure is being upgraded in 14,708 border villages in the Ladakh region, as part of the border area development plan (BADP). In 2020, the BADP guidelines were revised to cover villages from 0-50 km from the border. On completion of the project, Ladakh's strategically important remote locations, including Chumar and Demchuk, will get 4G internet connectivity. According to Union home ministry officials, efforts are being made to develop local government directory codes in 1,860 border villages, while the list of 14,708 villages has been shared with the DoT for developing telecom infrastructure.[8]

5G trials and connected issues

5G trials are on course, with all three telecom service providers in association with equipment vendors carrying out field trials across 13 city hubs, within the allocated trial spectrum. On December 23, trials for rural broadband began at a village in Gujarat, with a base transceiver station (BTS) installed 17 km away. Virtual-reality connected classrooms, 5G immersive gaming, and artificial intelligence assisted 360 degrees cameras with real-time video streams are being tested.

Adequate spectrum in the 5G bands is planned to be auctioned in 2022. There are, however, disputes with regard to spectrum allocation for telecom and satellite service providers. While the Committee of Secretaries is discussing various options, the Telecom Regulator (TRAI) has sought comments on setting base prices of 5G spectrum bands by January 24.

Amidst these trials, there have been positive developments with regards to standards. On December 13, it was formally accepted that the indigenous 5G Radio Interface Technology (RIT) called 5Gi, developed by the Telecommunications Standards Development Society, India (TSDSI) and the 5G standard of 3rd generation partnership program (3GPP) will be merged under a compromise formula. Earlier, 5Gi was to be deployed independently to provide last mile connectivity for enhanced coverage in rural areas of India, but

[8] 4G internet: Border villages along China border to have high-speed internet, Telecom News, ET Telecom (indiatimes.com)

it did not find much support due to technology fragmentation, rollout cost and interoperability challenges.

A key achievement of the merger for the 'made in India standard' is that the proposed features of 5Gi will now be globally deployed and any future development of 5Gi will happen under the aegis of 3GPP. The harmonisation of 5Gi with the global standard will also see certain changes in the configurations, including doubling of the power level in the devices and the modulation scheme. The merger will be a key enabler to achieve high-speed, high-quality inter-operable connectivity for all as 5G gets rolled out.[9] The merged technology 3GPP-5Gi has been evaluated by ITU so that it conforms with the International Mobile Telecommunications 2020 (IMT-2020) vision and stringent performance requirement set for 5G. It now awaits formal approval.[10]

In another positive development, 5G test beds are being launched in January 2022. On December 27, it was reported that the indigenous test bed project would pave the way for end-to-end testing of 5G user equipment and network equipment by small and medium enterprises and other industry players to test India based use cases. [A testbed consists of a specific environment including hardware, software, operating system, and network configuration to test a product or service.][11]

Notwithstanding these developments, challenges to develop infrastructure for the early roll out of 5G remain. In spite of India being the second largest internet user, low broad band penetration persists due to legacy rules pertaining to Right of Way (ROW) for laying optical fibre cables.[12] On December 25, TRAI issued a consultation paper on non-discriminatory and mandatory deployment of telecom infrastructure to effectively address the right-of-way (ROW) issues within building premises. Industry estimates suggest that nearly 70% of mobile traffic originates from indoors. This may require modifications in the Real Estate (Regulation and Development) Act, 2016, and the urban development framework.[13]

[9] 5Gi and 3GPP 5G Standards to be Merged (telecomtalk.info)
[10] https://www.itu.int/en/mediacentre/Pages/pr26-2020-evaluation-global-affirmation-imt-2020-5g.aspx
[11] Indigenous 5G testbed project: 5G services to be launched soon in 13 cities across India, Government News, ET Government (indiatimes.com)
[12] Bharatnet: Expedite RoW permissions to ensure broadband availability: K Rajaraman to state IT secretaries, Telecom News, ET Telecom (indiatimes.com)
[13] 5G: Telecom Diary: 5G remains talk of the town but infrastructure a big challenge, Telecom News, ET Telecom (indiatimes.com)

Incentives to boost Semiconductor Eco-system

Recognising the strategic importance of semiconductors for the security of national information infrastructure, on December 15 the Union Cabinet approved a ₹76,000 crore ($10 billion) scheme to boost semiconductor and display manufacturing, aimed at making India a global hub of electronic system design and manufacturing. The scheme will provide fiscal support of up to 50% of the project cost for setting up units to fabricate chips up to 28nm, 40% of the cost for chips from 28nm to 45nm, and up to 30% for chips above 45nm and up to 65nm. [nm or nanometre is one-billionth of a meter and in semiconductors, represents the least distance between transistors in a chip]. For fiscal support as equity, the government's share will not exceed 49 per cent of total project. Necessary infrastructure including land, power and semiconductor-grade water would be facilitated. The 'India Semiconductor Mission' will be the nodal agency to implement the scheme over six years.[14]

On December 3, Parliament was informed that semiconductor design is a highly knowledge-intensive field and needs exceptionally skilled manpower and tools. India has such resources in private and strategic sectors and a high number of design patents are produced in the country. Currently, semiconductor wafer fabrication facilities for strategic requirements are available at Semiconductor Laboratory (SCL), Mohali; Gallium Arsenide Enabling Technology Centre (GAETEC), Hyderabad and Society for Integrated Circuit Technology and Applied Research (SITAR), Bengaluru.[15] To harness Indian talent, the government has launched a "chips to start-ups" programme that will provide 50% of the expense of private start-ups, under the design-linked incentive scheme.[16]

Several major technology firms including Intel; Israel's Tower Semiconductor; Taiwan's TSMC, United Microelectronics Corp. and Foxconn; Korea's LG and Samsung; Japan's AvanStrate; a consortium from Singapore; and the Tata and Vedanta Groups, have shown interest in the scheme.[17]

Proposals for crypto regulatory framework

Blockchain technology is seeing greater adoption for a diverse range of services and use cases from Web 3.0, land record management, inventory

[14] Govt To Offer Up To 50% Of Project Cost To Cos Setting Up Chip Plant, Auto News, ET Auto (indiatimes.com)
[15] CHIP INDUSTRY: Govt has Rs 100 cr budget for chip design related activities this fiscal: IT Minister Ashwini Vaishnaw, Auto News, ET Auto (indiatimes.com)
[16] Union Cabinet approves ₹76,000-crore push for semiconductor makers - The Hindu
[17] Semiconductor Incentive: India's USD10 billion chip incentive: Which Singapore companies may jump in, Telecom News, ET Telecom (indiatimes.com)

management, financial services, Non-Fungible Tokens (NFTs), to healthcare and identity management solutions. On December 28, Prime Minister Narendra Modi launched blockchain-based digital degrees at the 54th convocation ceremony of Indian Institute of Technology (IIT), Kanpur. These digital degrees are unforgeable and may be confirmed globally.[18]

However, the best-known use case for blockchain is cryptocurrency - a tradable digital asset or digital form of money - that is built on decentralised technology. Venture capital funding worth $511 million was made in the cryptocurrency, blockchain and NFT ecosystem in 2021, but almost 90% of this went to crypto exchanges. WazirX, India's biggest Cryptocurrency exchange, registered an annual trade of over $43 billion. If properly regulated, the Government can tax the revenue being generated.[19]

Recognising the need to regulate cryptocurrencies, the Indian PM, while delivering India's "national statement" at the US Summit for Democracy on December 10, called for efforts by the international community to jointly shape global norms for emerging technologies like social media and crypto currencies so that "they are used to empower democracy, not to undermine it".

While the "Cryptocurrency and Regulation of Official Digital Currency Bill, 2021" has been deferred, industry bodies are active in suggesting regulatory frameworks and a code of conduct to sustain the cryptocurrency eco-system. On December 9, the Confederation of Indian Industries (CII) urged the government to treat cryptocurrencies as a special class of securities with a new set of regulations, keeping in mind their jurisdiction-less and decentralised character. Like CII, the IAMAI also pushed for cryptocurrencies to be classed as assets. In a submission before the Supreme Court last month, the IAMAI listed several negative outcomes of a blanket ban on crypto, such as zero accountability and traceability of the origin and end-use, besides a complete evasion of taxes.

On November 25, the Blockchain and Crypto Assets Council (BACC) suggested a smartly regulated crypto sector that would protect investors, help monitor Indian buyers and sellers, lead to better taxation of the industry, and curb the illegal use of crypto by non-state actors. It suggested that the government establish centralised exchanges under the Securities and Exchange Board of India (SEBI).

[18] https://www.the420.in/blockchain-based-digital-degrees-launched-by-pm-modi-at-iit-kanpur-convocation-ceremony/
[19] https://www.mondaq.com/india/fin-tech/1145012/cryptocurrency-bill-2021-the-road-ahead

Countries like Canada, Singapore and Switzerland, where cryptocurrencies and crypto-assets are legal, have strong regulatory frameworks that mandate know your customer (KYC) and Anti-Money Laundering (AML) mechanisms, and demand adherence to Combating Financing of Terrorism (CFT) requirements.[20]

Capability Building in Indian Army

On December 29, it was reported that the Indian Army has established a Quantum Lab at Military College of Telecommunication Engineering, Mhow (MP), with support from the National Security Council Secretariat (NSCS). Key thrust areas are Quantum Key Distribution, Quantum Communication, Quantum Computing and Post Quantum Cryptography. A multi-stakeholder approach has been adopted by incorporating Academia, DRDO organisations, Research Institutes, Start-ups and Industry. The Indian Army has also established an Artificial Intelligence (AI) Centre at the same institution. Training on cyber warfare is being imparted through a state of the art cyber range and cyber security labs.[21]

[20] crypto ban: Banning crypto would encourage non-state players, says industry body - The Economic Times (indiatimes.com)
[21] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1786012

International Developments

Ransomware attacks continue unabated

Even after high profile summit meetings and sanctions imposed on identified entities, ransomware attacks continue across the globe. On December 2, the US Federal Bureau of Investigation warned that a Cuba ransomware gang has compromised at least 49 entities in five critical sectors, including financial, government, healthcare, manufacturing and information technology, which have made $43.9 million in ransom payments to the group. The entities were infected by Hancitor, a malware operation that uses phishing emails, Microsoft Exchange vulnerabilities or compromised credentials as tools to gain access to vulnerable Windows systems. Once systems are added to their botnet, Hancitor operators rent access to these systems to other criminal gangs in a classic Malware-as-a-Service model.[22]

On December 6, an electric utility in Colorado was targeted in an apparent 'file encrypting' ransomware attack that resulted in significant disruption and damage. The Delta-Montrose Electric Association (DMEA) is a member-owned and locally controlled rural electric cooperative that serves more than 34,000 customers in Colorado's Montrose, Delta, and Gunnison counties.[23] On December 6, the Microsoft Digital Crimes Unit (DCU) disrupted the activities of a China-based hacking group called Nickel, based on directions of a federal court in Virginia to seize websites used to attack organisations in the United States and 28 other countries around the world. These attacks were largely being used for intelligence gathering from government agencies, think tanks and human rights organisations. Reportedly, there is often a correlation between Nickel's targets and China's geopolitical interests.[24]

Facebook deletes accounts of surveillance-for-hire firms

On December 16, Facebook owner Meta took down several accounts linked to seven "surveillance-for-hire" firms and notified about 50,000 people in more than 100 countries including journalists, dissidents and clergy who may have been targeted by them. 300 Facebook and Instagram accounts linked to one firm Cytrox were deleted. Cytrox, founded in Israel in 2019 to compete with the infamous NSO group, has customers in Egypt, Armenia, Greece, Indonesia, Madagascar, Oman, Saudi Arabia, and Serbia. Other firms targeted by Facebook

[22] FBI says the Cuba ransomware gang made $43.9 million from ransom payments - The Record by Recorded Future
[23] https://www.securityweek.com/cyberattack-causes-significant-disruption-colorado-electric-utility
[24] https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/

included four Israeli companies (Cobwebs, Cognyte, Black Cube, and Bluehawk), India-based BellTroX and an unknown Chinese firm. Evidence of the hacking was also cited by the Canada-based Citizens Lab on December 29,[25] whose report exposes the depth and diversity of the "surveillance-for-hire" industry that provides different kinds of surveillance activities, ranging from simple intelligence collection through fake accounts to wholesale intrusion.[26]

Some countries have taken measures to tighten oversight on these companies. NSO and Candiru have been put on an entity list that bars U.S. companies from providing them with technology. Israel's Defence Ministry has tightened oversight over cybersecurity exports to prevent abuse. Export control is also a key issue before the "Trade and Technology Council" between the US and the European Union. In the private sector, Apple and Meta have taken recourse to legal actions.

On December 14, it was reported by Bloomberg that following these actions, the NSO Group is exploring options that include shutdown of its Pegasus unit and sale of the company. Notwithstanding these developments, greater international efforts at the level of the United Nations are required to evolve global norms to curb the menace of abusive surveillance by such "surveillance-for-hire" entities.

Log4j vulnerabilities affect the Global internet

On December 17, the US Cybersecurity and Infrastructure Security Agency (CISA) warned that a vulnerability in Java-based software known as "Log4j" has affected the global internet. Log4j is a logging library that assists software developers in a variety of purposes, such as troubleshooting, auditing and data tracking. Exploiting this vulnerability gives an adversary deep access into a target network, allowing them to exfiltrate information or cause other harmful attacks.[27]

On December 14, in its blog post on the log4j vulnerability, Microsoft warned that its Threat Intelligence Center (MSTIC) had seen evidence of nation-state hacking groups in China, Iran, North Korea and Turkey exploiting it. While Microsoft did not name the threat actors, on December 29 security researchers

[25] pegasus: Poland spyware cases 'tip of the iceberg': watchdog, IT Security News, ET CISO (indiatimes.com)
[26] spyware: Spyware find highlights depth of hacker-for-hire industry, IT Security News, ET CISO (indiatimes.com)
[27] https://thehill.com/policy/cybersecurity/585904-china-iran-among-those-seen-exploiting-apache-cyber-vulnerability

linked Log4Shell attacks to threat actors including the Iran linked "Phosphorous" and Chinese groups "Aqua Panda" and "Hafnium", which exploited flaws in Microsoft's Exchange Server to attack academic entities.[28]

Australia to regulate crypto and BNPL

On December 6, Australia proposed a licensing framework for cryptocurrency exchanges and a retail central bank digital currency (CBDC). The country will also broaden its payment laws to cover online transaction providers like Apple Inc and Alphabet Inc's Google as well as buy-now-pay later (BNPL) providers like Aftearpay Ltd. The Framework proposes the purchase and sale of crypto assets by consumers in a regulated environment and regulates BNPL companies to address the risk of debt and financial stress associated with these products. The move would represent the biggest overhaul of Australia's $463 billion-a-day payments industry in 25 years.

The Framework is in line with global efforts to rein in large technology companies, amid a surge of 63% in the use of cryptocurrencies and non-cash payments during the Covid-19 pandemic. It is akin to the U.S. and UK proposals for regulatory frameworks that to allow banks to facilitate ownership of crypto assets for customers while giving powers to regulators to govern the online promotion of crypto assets.

At the other end of the spectrum, India's proposed Bill calls for a possible ban of private crypto currencies and the launch of a retail CBDC, while Chinese regulators have already banned both crypto transactions and mining.[29]

UK publishes standard for algorithmic transparency

On December 29, the UK government launched its first national standard for algorithmic transparency which strengthens the UK's position as a global leader in trustworthy AI. The standard is based on a review by its Centre for Data Ethics and Innovation (CDEI) into bias in algorithmic decision-making and its recommendations to place a mandatory transparency obligation on public sector organisations using algorithms to support significant decisions affecting individuals. It delivers on stipulations in the National AI Strategy and National Data Strategy to bring necessary scrutiny to the role of algorithms in decision-making processes, and help build public trust.

[28] Log4Shell attacks expand to nation-state groups from China, Iran, North Korea, and Turkey - The Record by Recorded Future

[29] crypto news: Australia proposes new laws to regulate crypto, BNPL - The Economic Times (indiatimes.com)

The standard will be piloted by several public sector organisations in the UK. Based on feedback, the Central Data Digital Office (CDDO) will review it further and seek the formal endorsement of the UK Data Standards Authority during 2022.[30]

UK Launches National Cyber Strategy 2022

On December 15, the UK launched its National Cyber Strategy 2022 with a vision that the UK in 2030 will continue to be a leading, responsible and democratic cyber power, able to protect and promote its interests in and through cyberspace in support of its national goals. To realise this vision, it sets out five strategic goals/pillars to guide its activities in cyberspace. These include strengthening the UK cyber ecosystem, investing in people and skills and deepening the partnership between government, academia and industry; building a resilient and prosperous digital UK, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are secure online and confident that their data is protected; taking the lead in the technologies vital to cyber power, building industrial capability and developing frameworks to secure future technologies; advancing UK global leadership and influence for a more secure, prosperous and open international order; working with government and industry partners and sharing the expertise that underpins UK cyber power; and finally detecting, disrupting and deterring adversaries to enhance UK security in and through cyberspace, making more integrated, creative and routine use of the UK's full spectrum of levers.[31]

To count itself as a leading Cyber Power, the UK has invested in capabilities and skills to build on cyber defence and resilience. The lead Cyber agency is the National Cyber Security Centre - a part of GCHQ - that partners with private and public sectors to respond to incidents, warn of threats and offer tailored advice and guidance to stay safe online. Alongside this defensive posture, it has continued to build offensive cyber capability. The UK National Cyber Force is a partnership between intelligence and the MOD that conducts cyber operations with other aspects of statecraft across the entire spectrum of national security. These capabilities enable the UK, "legally and proportionately, to contest and challenge malign states and criminals in cyberspace". The Strategy focusses on

[30] UK government publishes pioneering standard for algorithmic transparency - GOV.UK (www.gov.uk)

[31] https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

geo-political competition due to technologies and includes collaboration with allies, partners and industry to set technology standards that govern it.[32]

India is in the process of finalising its National Cyber Security Strategy. It will be good for policy makers to study the UK Strategy and compare and adapt relevant clauses that suit India's national interest.

[32] https://www.gchq.gov.uk/pdfs/speech/national-cyber-strategy-2022.pdf

International Cooperation

India-Russia Joint Statement regarding digital security

On December 6, the Russian President and the Indian Prime Minister met for the 21st India-Russia Annual Summit. In the Joint Statement issued thereafter, both sides appreciated close cooperation in the field of security in the use of Information and Communication Technologies (ICT) through inter-agency cooperation under bilateral mechanisms and at multilateral platforms. They highlighted the leading role of the United Nations in the decision-making process on security in the use of ICTs. They also recognised the need for further work on rules, norms and principles of responsible behaviour of States aimed at preventing conflicts and promoting peaceful use of ICTs. They reaffirmed the importance of international cooperation against criminal use of ICTs and welcomed the establishment of an open- ended intergovernmental committee of experts to elaborate a comprehensive international convention on countering the use of ICTs for criminal purposes as stipulated in the UNGA resolutions 74/247 and 75/282.

The two sides further agreed to facilitate collaboration between government and private sector organisations for joint development of software products, platforms and services as well as in the area of electronics manufacturing. They confirmed their interest in further developing cooperation in the sphere of digital technologies, including those related to information protection, security of critical infrastructure and law enforcement.[33]

India-ITU Joint Cyber drill 2021

On December 3, India and International Telecommunication Union (ITU) successfully completed India-ITU Joint Cyber drill 2021, under the aegis of Department of Telecommunications. Panellists and experts from international organisations including ITU, UNODC, and INTERPOL, along with representatives from industry and security agencies, deliberated on international best practices and global policy initiatives on cybersecurity. Ms Atsuko Okuda, Director of ITU's Regional Office for the Asia and Pacific Region, highlighted the significant achievement of India in securing 10th rank in the ITU Global Cybersecurity Index (GCI). More than 400 professionals representing all stakeholders participated in the Drill to deepen operational

[33] India- Russia Joint Statement following the visit of the President of the Russian Federation (mea.gov.in)

cooperation on cyber security and protection of critical information infrastructure.[34]

***

[34] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1776732

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

www.delhipolicygroup.org