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

DPG CYBER REVIEW

NOVEMBER 2021

Volume II, Issue 11 | November 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 11
November 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

© 2021 by the Delhi Policy Group

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

DPG Cyber Review
Vol. II, Issue 11
November 2021

Contents

Abstract

The month began with an aggressive social media campaign from China threatening military action in the Tawang sector, with fake videos and photos of People's Liberation Army (PLA) troops. While India has seen a 261 percent increase in Chinese-backed cyber-attacks, Chinese State Media blamed India for several attacks targeting government and military enterprises in China, Pakistan, and Nepal.

The National Cyber Security Coordinator is steering a project called Indian Citizens Assistance for Mobile Privacy & Security (I-CAMPS), in a public-private collaboration, to identify privacy and security issues in mobile phones. The 'Personal Data Protection Bill 2019' and the 'Cryptocurrency and Regulation of Official Digital Currency Bill, 2021' are slated to be tabled during the Winter session of Parliament. With the ongoing trials and impending rollout of 5G, Indian innovators are also exploring 6G technology. India will adopt IPV6 internet address which will facilitate 5G technology-backed adoption of Internet of Things (IoT).

Several measures are being taken by the US and Europe aimed at criminal gangs and crypto currency exchanges which have been behind ransomware attacks that have crippled critical infrastructure and businesses. Separately, a joint Cybersecurity Advisory was issued by the US, Australia and UK highlighting "ongoing malicious cyber activity by an advanced persistent threat (APT) associated with the government of Iran". Taiwan's defence ministry warned that Chinese hackers had infiltrated at least 10 Taiwan government agencies and gained access to around 6,000 email accounts in an attempt to steal data.

The U.S. President signed the ''Secure Equipment Act 2021" during the month to ban Chinese tech companies on US networks, while the Australian PM announced a Bill to make social-media companies liable for defamatory comments published on their platforms. China's Personal Information Protection Law (PIPL), regulating transfer of data outside China's borders, took effect from November 1.

The first meeting of the India-UK Joint Working Group on Cyber Deterrence was held in virtual mode to step up bilateral cooperation for building effective cyber deterrence strategies.

UNESCO has unanimously adopted comprehensive recommendations to provide Artificial Intelligence (AI) with a strong ethical basis, which are

intended to protect and promote human rights and contribute to the achievement of the sustainable development goals.

National Developments

Cyberattacks by South Asian adversaries

Amid tensions along the LAC in the Eastern Sector and establishment of "a large 100-home civilian village inside disputed territory between the PRC's Tibet Autonomous Region and India's Arunachal Pradesh", as indicated in the US DOD's 'Annual Report to Congress: Military and Security Developments Involving the People's Republic of China',[1] China unleashed a propaganda and psychological warfare campaign on social media. As reported on November 7, Chinese entities initiated an aggressive social media drive threatening military action in Arunachal Pradesh, with several Twitter handles releasing fake videos and photos of People's Liberation Army (PLA) troops at the eastern front of the LAC, targeting Tawang.[2]

It was reported on November 5 that India had witnessed an estimated 4,90,000 cyberattacks originating from Pakistan during the India-Pakistan cricket match at the T20 World Cup on October 24. This was the first time that such cyberattacks have been linked to a sports event involving subcontinent teams. A few IP addresses from South East Asia and Eastern Europe linked to hijacked botnets[3] were also found to be participating in these attacks on India.

On November 21, the Chinese paper Global Times reported that an active hacker group in Delhi has been launching cyberattacks against government agencies and defense departments. It alleged that these Indian hacking groups (called 'Baby Elephant', 'Evil Flower', 'White Elephants' etc.) were linked to the Indian State and had carried out multiple cyberattacks on government and military enterprises in China, Pakistan, and Nepal.[4] The Global Times quoted a Chinese anti-virus company, Antiy Labs, to allege that more than 100 phishing counterfeit websites have been found which target major universities, state-owned enterprises and key organs of the government in China.

India has seen a 261 per cent annual increase in Chinese-backed cyberattacks as of August 2021. China has been deflecting the blame by accusing India of

[1] DOD 2021 Report on Military and Security Developments Involving the People's Republic of China (defense.gov)

[2] Mission Tawang: PLA Army Heading Towards India's Arunachal Pradesh; Will Seize Key Disputed Points: Chinese Social Media (eurasiantimes.com)

[3] 4.9 lakh cyberattacks from Pakistan targeted India during 24 October T20 World Cup match (theprint.in)

[4] Exclusive: New hacker group from India exposed, targeting defense units in China, Pakistan - Global Times

hacking attempts through its State-owned newspapers, as indicated in the preceding para.

Project to address privacy and Security in mobile phones

On November 8, the National Cyber Security Coordinator launched a new project to identify privacy and security issues in mobile phones. The National Security Council Secretariat (NSCS) is collaborating with various government departments for the project called "Indian Citizens Assistance for Mobile Privacy & Security (I-CAMPS)". The project's aim is to build an integrated system which can collate all the mobile security related information and provide customized and actionable knowledge to individual Indian citizens to secure their mobile devices and data on those devices. The Internet and Mobile Association of India (IAMAI) has been tasked to execute this project in collaboration with device makers, service providers and App providers as well as government stakeholders dealing with various aspects of mobile management, security and governance.[5]

NCSC has also been tasked to designate 'trusted' telecom sources and products under the National Security Directive on the Telecommunication Sector (NSDTS). The Apex Cyber Security Organisation should as a result get suitably augmented to take on these multi-faceted tasks.

Data Protection Bill on the anvil

The above initiative to protect mobile privacy comes in the midst of reports that the Joint Committee of Parliament, which is examining the Personal Data Protection Bill 2019, has adopted the Bill with a few dissent notes. Most dissents pertain to Section 35, which exempts Central government agencies from its provisions in the interest of national security, public order, sovereignty and integrity of India, and friendly foreign relations, without oversight. Another point of dissent has been on the inclusion of non-personal data within its ambit, which may change the nature of the Bill. The Bill also reportedly seeks registration of companies dealing with children's data with the Data Protection Authority which will have powers to decide on implementing the law's various provisions. The Bill was drafted following a Supreme Court judgement in 2017 that recognised privacy as a fundamental right of Indian citizens. It will now be tabled during the winter session of Parliament.[6]

[5] ncsc: India's security coordinator kicks off new project to identify privacy, security issues in mobile phones, apps, Telecom News, ET Telecom (indiatimes.com)

[6] data protection bill: Parliamentary panel adopts report on data protection bill - The Economic Times (indiatimes.com)

New cryptocurrency bill in the offing

Another significant legislation likely to come up during the Winter Session of Parliament is the "Cryptocurrency and Regulation of Official Digital Currency Bill, 2021". On November 23, the Lok Sabha Bulletin mentioned the Bill for introduction, consideration and passing. The purport of the Bill is to create a facilitative framework for creation of the official digital currency to be issued by the Reserve Bank of India. The Bill also seeks to prohibit all private cryptocurrencies in India; however, it allows certain exceptions to promote the underlying technology of cryptocurrency and its uses.[7] The cryptocurrency market has been growing exponentially over the last few years and is expected to reach up to $241 million by 2030 in India and $2.3 billion by 2026 globally.[8]

The Bill is being tabled amid concerns that private crypto currencies played a significant role in escalating ransomware attacks across the globe. On November 22, the Parliamentary Standing Committee on Finance discussed the issue of crypto finance with various stakeholders. It is reported that regulating crypto currency exchanges found greater favour rather than an outright ban, to prevent youth from being misled through over-promising and non-transparent advertising of crypto currencies. Exact contours of the Bill are not in the public domain.[9] On November 29, the Finance Minister stated in Parliament that the government has no proposal to recognise the private crypto currency-Bitcoin as a currency in the country. She also informed the House that the government does not collect data on Bitcoin transactions.[10]

5G trials and the Launch of 6G

India has been slow in creating its own technology standards. As a result, the lone indigenous 5Gi technology approved by the ITU is being promoted for adoption during 5G trials. However, telecom service providers have reservations on its adoption on grounds of interoperability with global 3GPP standard compliant devices and commercial viability. To address the issue, on November 2, The Department of Telecommunications (DoT) formed a committee to chart out a strategy for the commercialisation and monetisation of 5G and the adoption of the locally developed 5Gi standard.[11]

[7] http://loksabhadocs.nic.in/bull2mk/2021/23.11.21.pdf (page12, Serial10)

[8] Indian cryptocurrency market likely to reach up to $241 million by 2030: Nasscom - The Hindu BusinessLine

[9] New cryptocurrency bill seeks to ban private players - The Hindu

[10] No proposal to recognise Bitcoin as a currency: FM Sitharaman - The Economic Times (indiatimes.com)

[11] Department of Telecommunications: DoT forms committee to chart out strategy for commercialization of 5G & local 5Gi: Report, Telecom News, ET Telecom (indiatimes.com)

The Government is also working to fast track the auction of 5G spectrum in the second quarter of 2022. The consultative process with the Telecom Regulatory Authority of India (TRAI) for 5G spectrum auctions is currently under progress. In September, the Cabinet had approved a set of nine structural and procedural reforms to address the short-term liquidity needs as well as long-term issues of telecom companies, including issues related to spectrum auction.

With the ongoing trials and impending rollout of 5G, Indian innovators are also exploring the 6G technology that will reshape the way people interact with Artificial Intelligence. On November 23, the Minister for Communications stated that India is working towards an indigenously developed 6G technology which is likely to be launched by early 2024. India is collaborating with Finland under a digital partnership that will focus on the development of 6G technology and the use of digital tools to transform education.[12]

The growth in the number of devices connecting to the internet, with the adoption of these technologies, has fueled demand for more internet protocol (IP) addresses, which help in identifying and connecting various devices and servers onto the internet. Consequently, the adoption of the IPV6 is being hastened. On November 2, DOT revised the timeline for the transition to Internet Protocol version 6 (IPv6) to December 31, 2022. Internet service providers are required to customise their network and change modem and routers accordingly. The DoT has also set June 30, 2022, as the last date for government organisations for complete transition to IPv6.[13]

The revised timeline would address the need for more Internet addresses following the 5G technology-backed adoption of Internet of Things (IoT), as the current version of Internet Protocol (IPv4) has almost run out of addresses. IPv6 uses a 128-bit addressing system and can support up to 340 trillion devices. India currently ranks highest with a 61.23% IPv6 adoption rate worldwide.[14]

At present, there are 13 root servers globally, with none in India, that play a vital role in the internet. With the adoption of IPv6 addresses, with inbuilt security features, India can set up its own root server for the internet. This has been a long-standing security requirement for 5G/6G communications within the country's geographical boundaries.

[12] 6G technology launch likely by 2023-end or 2024, says Ashwini Vaishnaw | Technology News,The Indian Express
[13] DoT Fixes December 2022 Deadline For Transition To New IP Addresses (moneycontrol.com)
[14] dot IPv6: DoT's new IPv6 transition timelines to hasten adoption: Forum, Telecom News, ET Telecom (indiatimes.com)

Forays into Semiconductor Chip manufacturing

It was reported on November 26 that India’s Tata Group is in talks to set up a $300 million semiconductor assembly unit. The company is reportedly scouting for land for the outsourced semiconductor assembly and test (OSAT) plant. An OSAT plant packages, assembles and tests foundry-made silicon wafers, turning them into finished semiconductor chips. Potential clients of Tata's OSAT business include companies such as Intel, Advanced Micro Devices (AMD), and STMicroelectronics. The move will boost India’s ‘Make in India' drive for semiconductor chip manufacturing.[15]

[15] Tata Group: India's Tata in talks to set up $300 million semiconductor assembly unit, Telecom News, ET Telecom (indiatimes.com)

International Developments

Global Crackdown on Ransomware attacks

On November 22, it was reported that 79 per cent of global cybersecurity incidents in the last 18 months were ransomware attacks, led by "Ransomware-Evil", or REvil, and aided by cryptocurrencies.[16] To curb the menace, law enforcement authorities in the U.S. and Europe announced a series of actions in November, aimed at criminal groups behind ransomware attacks that crippled critical infrastructure and businesses.

On November 4, the US Department of State offered up to a $10 million reward for information leading to the identification or location of senior members of the DarkSide gang that caused major gas supply disruptions earlier this year. In addition, the U.S. State Department is offering a reward of up to $5 million for information leading to the arrest and/or conviction in any country "of any individual conspiring to participate in or attempting to participate in a DarkSide variant ransomware incident."[17]

In Europe, the European Union's law enforcement agency – Europol – arrested two suspects in Romania on November 4, as part of Operation 'GoldDust', partnered by 17 countries including the US, the UK, France, Australia and Germany, to investigate ransomware attacks. The suspects had allegedly extorted an estimated 500 million euros from companies for restoring over 5000 computer systems infected with REvil ransomware. Five hackers linked to REvil and responsible for most cyberattacks have been arrested since February.[18]

On November 8, the US Treasury Department imposed sanctions on cryptocurrency exchange Chatex for "facilitating financial transactions for ransomware actors." Over half of Chatex transactions are traced to illicit or high-risk activities such as darknet markets, high-risk exchanges, and ransomware. Chatex exchange reportedly has "direct ties" to a Russian cryptocurrency exchange Suex, which was sanctioned in September.[19] Further,

[16] US Treasury Sanctions Crypto Exchange in Anti-Ransomware Crackdown | SecurityWeek.Com

[17] US Offers $10 Million Bounty in Hunt for DarkSide Ransomware Operators | SecurityWeek.Com

[18] europol: Five hackers linked to ransomware gang REvil arrested since Feb -Europol, IT Security News, ET CISO (indiatimes.com)

[19] US Treasury sanctions crypto-exchange Chatex for links to ransomware payments - The Record by Recorded Future

the US Justice Department charged two operatives from Ukraine and Russia, and seized $6 million in ransom payments.[20]

Iranian hackers named in alleged Cyberattacks

On November 17, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Australian Cyber Security Centre (ACSC), and the U.K.'s National Cyber Security Centre (NCSC) released a joint Cybersecurity Advisory highlighting "ongoing malicious cyber activity by an advanced persistent threat (APT) associated with the government of Iran". Hackers had reportedly exploited Microsoft Exchange vulnerabilities to gain initial access to computer systems for follow-on activities, including data exfiltration and ransomware.[21]

This was followed by sanctions against six Iranian nationals and an Iranian cyber-company for "attempting to influence" last year's US presidential elections, between August and November 2020. The US Treasury Department accused the sanctioned individuals and company of disseminating disinformation on social media and sending threatening emails and a fraudulent video that sought to "undermine faith in the election by implying that individuals could cast fraudulent ballots".[22]

Separately, on November 19, U.S. authorities charged two Iranian nationals of cyber-related crimes allegedly carried out to engage in voter intimidation and election interference ahead of the 2020 US presidential election. The Treasury Department sanctioned the pair along with four other Iranian nationals, describing them as "state-sponsored actors" involved in a disinformation campaign. It was reported that hackers infiltrated the computer systems of Lee Enterprises Inc., a major American media company, to create false news content as part of a broader effort to spread disinformation about the 2020 presidential election.[23]

Iranian hackers are also reportedly targeting Indian IT service firms and the frequency of attacks has escalated since July 2021. On November 18, Microsoft warned in its blog that it has issued 1,788 nation-state notifications or NSNs to its enterprise customers, of which 80 per cent were IT companies, mostly from

[20] U.S. charges Ukrainian, Russian, over cyberattack, seizes $6 mln in ransom payments, IT Security News, ET CISO (indiatimes.com)

[21] Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities | CISA

[22] Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election | U.S. Department of the Treasury

[23] Iranian Hackers Broke Into Newspaper Publisher Lee Enterprises Ahead of 2020 Election - WSJ

India. As India rises as a major IT services hub, nation-state actors follow the supply chain to target these backend infrastructures of the top global companies to gain indirect access to customer networks outside India. "The Microsoft Threat Intelligence Center (MSTIC) and Digital Security Unit (DSU)" regards this as part of a broader espionage objective to compromise organisations of interest to the Iranian regime."[24]

Cyber Capabilities of China impacting Taiwan

On November 9, Taiwan's defence ministry warned that its information security and protection centre detected and handled around 1.4 billion "anomalies" from 2019 to August 2021 to prevent potential hacking. The related report warned that China has been "vigorously enhancing" its cyber warfare capabilities as part of the strategy to bring the island to heel. Taiwan's government agencies face around "five million cyberattacks and scans every day", as disclosed in Taiwan Parliament. Chinese hackers infiltrated at least 10 Taiwan government agencies and gained access to around 6,000 email accounts in an attempt to steal data.[25]

A recent Pentagon report on China's increased military capacities has singled out Beijing's growing cyber capabilities as a destabilising factor that can impact the fragile peace in the Asia Pacific. PLA writings advocate strong cyber capabilities to seize cyberspace superiority by using offensive cyber operations to deter or degrade an adversary's ability to conduct military operations against the PRC, including during peacetime.[26] To address the challenge, cyber security needs to be at the top of the agenda of regional and democratic partners and allies.

US addresses security concerns in cyber space

On November 11, U.S. President Joe Biden signed the "Secure Equipment Act 2021" to ban Chinese tech companies from getting approval for network equipment licences in the country. The legislation, that enjoyed bipartisan support, names telecom providers Huawei Technologies Co. and ZTE Corp., as well as radio-systems manufacturer Hytera Communications Corp. and video-surveillance companies Hangzhou Hikvision Digital Technology Co. and Zhejiang Dahua Technology Co., as deemed security threats. The new law requires the Federal Communications Commission (FCC) to no longer review

[24] https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/

[25] https://www.24newshd.tv/10-Nov-2021/taiwan-government-faces-5-million-cyber-attacks-daily-official

[26] DOD 2021 Report on Military and Security Developments Involving the People's Republic of China (defense.gov)

or approve any authorization application for equipment that poses an unacceptable risk to national security. The FCC has already authorized a $1.9 billion program to remove and replace equipment from Huawei and ZTE across the United States.[27]

In October, the FCC Commissioner had also warned that Chinese drone maker DJI "is collecting vast troves of sensitive data on Americans and US critical infrastructure, potentially operating as Huawei on wings". Shenzhen-based DJI accounts for more than 50 per cent of the US drone market.[28]

Semiconductors at the core of US-China tech war

US-China technology war is playing out globally by way of incentives, investments, subsidies and regulations to retain technological edge. Several Chinese tech companies have been added to the US Entity List, which prohibits them from sourcing US-origin technology without prior approval, ostensibly to prevent advanced chips from getting into the hands of China's military. In September, Washington asked major chipmakers and automakers using US technology to share supply chain data to better understand the global chip shortage. It had set a November 8 deadline for submission of information, which has triggered industry concerns over trade secrets. This has been followed up by placing restrictions on South Korean chipmaker, SK Hynix, from bringing in advanced machines to its chip fabrication plant in Wuxi, China. Consequently, the memory chip giant, had to scrap plans to install extreme ultraviolet lithography (EUV) scanners from Dutch firm ASML, that are required for producing cutting-edge 5- and 7-nanometre node chips. On November 22, the US Trade Representative remarked that "there are legitimate concerns about the risks to national security in terms of where this technology ends up." China has however, accused the US of conducting “chip hegemony” for its own profit. Similarly, China has tightened regulatory norms to deny its market to US companies.[29]

There have been a series of onshore semiconductor investments as part of the US strategy to reduce its reliance on sourcing advanced chips from Asia, mainly from Taiwan or China. On November 22, the US and Taiwan agreed to promote supply chain security and cooperate on semiconductors amid the global chip shortage. Separately, TSMC and Samsung have been provided incentives to

[27] https://www.reuters.com/technology/biden-signs-legislation-tighten-us-restrictions-huawei-zte-2021-11-11/

[28] Biden signs law to ban Huawei, ZTE from doing business in US - DTNext.in

[29] Taiwan Semiconductor Manufacturing Co: TSMC says it did not release any detailed customer data in response to US request, Telecom News, ET Telecom (indiatimes.com)

invest in new wafer fabs in the US. Subsidies are also being offered to US companies to bring their companies on shore.[30]

On November 8, it was reported by the Nikkei newspaper that Japan will create a scheme to subsidise construction of domestic chip factories with a new plant planned by Taiwan's TSMC in a joint venture with Sony's semiconductor subsidiary. The Japanese government is likely to subsidise up to half of TSMC's estimated 1-trillion-yen ($8.82 billion) investment for building a chip plant in Kumamoto, southern Japan. The plant is expected to produce semiconductors for automobiles, camera image sensors and other products which have been hit by a global chip shortage. Companies will be eligible for the subsidies on condition they ramp up chip production in times of short supply.[31]

Australian legislation on social media

On November 28, Australia announced that it would introduce legislation to make social-media companies liable for defamatory comments published on their platforms. The Australian Prime Minister stated that the "legislation would aim to unmask people who make hurtful comments online" by requiring social media companies to disclose their email address or cellphone number, when a complaint is made. The proposed legislation comes after a September ruling of the High Court of Australia determined that news organisations are legally liable for comments on their Facebook pages. According to the court, media companies are responsible for any defamatory content that appears on their Facebook pages because they are considered publishers of the comments. Social-media companies that provide those details, when a complaint is made, would have a defence from being the publisher of comments on their platforms. The proposed legislation is likely to be introduced in the Australian Parliament next year.[32]

China's Personal Information Protection Law takes effect

China's Personal Information Protection Law (PIPL), ratified on August 20, officially took effect on November 1. According to the legislation, multinational corporations will now have to obtain authorisation from government institutions to transfer data outside of China's borders. PIPL's "extraterritorial aspect" will also apply to non-PRC companies processing and/or analysing data belonging to Chinese users. With the regulatory and punitive measures in

[30] SK Hynix: US restriction on SK hynix plan in China 'legitimate': Trade chief, Telecom News, ET Telecom (indiatimes.com)

[31] global chip shortage: Japan to create scheme to subsidise domestic chip output, Auto News, ET Auto (indiatimes.com)

[32] Australia Seeks to Make Social-Media Firms Liable for Users' Defamatory Comments - WSJ

force, China's Ministry of Industry and Information Technology (MIIT) has sent notices to 38 apps, including the Tencent News, dating app Tantan, and social media platform Xiaohongshu, for collecting excessive personal data. The law will have major implications for companies that rely on data for their operations in China.[33]

Israeli Firm NSO Group faces legal strictures

On November 3, the US government added Israel's NSO Group and Candiru, alongside Russian cybersecurity firm Positive Technologies and Singapore-based Computer Security Initiative Consultancy Pte, to its Entity List, based on evidence that these companies developed and supplied spyware to foreign governments that used these tools to maliciously conduct transnational surveillance that threatens the rules-based international order. In a statement, the US Secretary of Commerce declared that "the United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations here and abroad."[34]

On November 23, Apple sued the NSO Group in a federal court. Earlier, Facebook had sued NSO in 2019 for targeting its WhatsApp users. Apple sought to hold NSO accountable for the surveillance and targeting of Apple customers and products using the Pegasus surveillance tool, "without effective accountability", that came to light in an investigative report in July. Apple requested a permanent injunction restraining Defendants from accessing and using any Apple product or service, besides seeking compensatory and punitive damages. NSO had created over 100 Apple IDs to carry out its alleged surveillance on customers.[35] The NSO representative reiterated that the company "provides governments the lawful tools to fight Paedophiles and terrorists who operate in technological safe-havens".

[33] https://www.cfr.org/blog/cyber-week-review-november-5-2021

[34] Explained: The significance of US putting NSO Group on its Entity List | Explained News,The Indian Express

[35] file:///C:/Users/DPG/Downloads/Apple_v_NSO_Complaint_112321.pdf

International Cooperation

UNESCO adopts AI ethics rules

There has been a global desire to introduce binding rules for Artificial Intelligence (AI) practices like social scoring and facial recognition in public places that are seen to endanger human rights and civil liberties. The U.N.'s Educational, Scientific and Cultural Organization's (UNESCO) is the first international organization to obtain unanimous support for the end of pervasive mass surveillance using AI.

On November 24, UNESCO adopted comprehensive recommendations to provide AI with a strong ethical basis, protect and promote human rights, contribute to the achievement of sustainable development goals, and build a strong respect for the rule of law in the digital world. UNESCO called on technologists to conduct ethical impact assessments, and on governments to put in place "strong enforcement mechanisms and remedial actions" to protect human rights. It also urges governments to dedicate public funds to promote diversity in technology in its assessments to protect indigenous communities and monitor the carbon footprint of AI technologies. UNESCO recommendations also include provisions on ensuring that real-world biases are not replicated online.[36] The USA is not a party to the recommendation, as it is no longer a member of UNESCO.[37]

India urges norms of internet governance

On November 25, the inaugural India Internet Governance Forum 2021 (IIGF21) recognised the importance of the Internet for economy and society. It urged the international community to define its norms of governance that would help to bridge the digital divide and focus on the goal of making the internet open, safe, trusted and accountable for all. The Internet need to be governed by open societies with the same set of democratic values and citizen's rights. The India Internet Governance Forum (IIGF 21) is an initiative associated with the UN Internet Governance Forum (UN-IGF), that brings together multistakeholder groups to discuss public policy issues, in conformity with the 2005 Tunis Agenda of the UN.[38]

[36] Recommendation on the ethics of artificial intelligence (unesco.org)

[37] https://www.e-ir.info/2019/02/14/why-did-the-u-s-and-israel-leave-unesco/

[38] https://pib.gov.in/PressReleseDetail.aspx?PRID=1775597 November 27, 2021

India-UK Joint Working Group on Cyber Deterrence

On November 25, the first meeting of the India-UK Joint Working Group on cyber deterrence was held in virtual mode. India and the UK agreed to work closely and hold regular consultations on addressing the challenges to cyber deterrence and for building effective cyber deterrence strategies. Both sides discussed ways to further deepen the existing bilateral cyber cooperation under the India-UK Framework for the Cyber Relationship concluded on April 17, 2018 in New Delhi.[39]

US-Israel joint task force on cybersecurity

On November 15, the United States and Israel announced a joint task force focused on ransomware. The partnership between the U.S. Treasury Department and their Israeli counterparts will see the two sides working to develop a Memorandum of Understanding supporting cybersecurity threat intelligence related to the financial sector, as well as cross-border cybersecurity exercises linked to global financial institutions' financial and investment flows. Both Israel and the United States are dealing with the rising threat of Iranian malware, and the US has recently detected an Iranian ransomware campaign directed against its critical infrastructure. The announcement follows a virtual meeting on ransomware that was held at the White House in October with the participation of more than 30 countries, including India.[40]

Sydney Dialogue and Bengaluru Technology Summit

The Sydney Dialogue for emerging, critical and cyber technologies and the Bengaluru Technology Summit, both held on November 17-19, helped to understand the complementary initiatives being undertaken by India, Australia and other QUAD partners. At the Sydney Dialogue, the Indian Prime Minister delivered the keynote, spoke on India's technology evolution and recounted five important transitions taking place in India. The address by the Indian PM was seen as a recognition of India's central role in the Indo Pacific region and in the emerging digital world.[41] The Bengaluru Tech Summit similarly fostered international engagement across technological domains. The Prime Ministers of Australia and Israel addressed the Summit virtually.[42]

[39] First Meeting of the India-UK Joint Working Group on Cyber Deterrence (mea.gov.in)
[40] U.S. to partner with Israel to combat ransomware attacks | Reuters
[41] https://pib.gov.in/PressReleseDetail.aspx?PRID=1772806
[42] https://www.bengalurutechsummit.com/

DPG

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

www.delhipolicygroup.org