Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

OCTOBER 2021

Volume II, Issue 10 | October 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 10
October 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 10
October 2021

Contents

Abstract

Developments during the month point towards increased phishing attacks and technical support scams on Indian enterprises. India stands sixth in the list of 140 countries most affected by ransomware. The long awaited National Cyber Security Strategy, to address growing cyberattacks, is nearing finalisation. 5G trials, along with the recent telecom reforms including production linked incentives, are transforming India's telecom landscape. Rational allotment of spectrums to all stake holders including satellite and telecom players will play a significant role in the early roll out of 5G.

In a significant judgment, the Supreme Court appointed a 3-member expert technical committee overseen by a former Supreme Court judge to examine allegations of surveillance using Pegasus spyware. The court's decisions on remedial measures will be significant.

The government is looking at rolling out a five-year strategic perspective plan to make India a significant technology player.

The menace of ransomware attacks continues with the reemergence of Russian hackers involved with the SolarWinds attacks, forcing major like-minded economic powers to collaborate on response. Recent cyber-attacks have hit Iran's fuel system and an Israeli hospital.

LinkedIn announced its decision to quit China due to a challenging operating environment and greater compliance requirements. It will continue to provide a stripped-down version of its application to help China's job market.

Whistleblower Frances Haugen exposed bias in Facebook processes affecting mental-health and political discourse, highlighted its inability/reluctance to prevent hate and fake messages, and suggested that that Facebook prioritised profit over consumer safety. Amidst this controversy, Facebook rebranded itself as 'Meta', signifying its focus on Metaverse as the new social media platform. Simultaneously, former U.S. president Donald Trump announced the launch of a new social media platform 'TRUTH Social' to stand up to Big Tech platforms.

The US administration held a meeting with representatives from 30 countries, including NATO allies, EU and G7 partners, to discuss methods to combat ransomware.

It was reported that Russia and the US have developed a UN General Assembly draft resolution on cybersecurity, based on the 2021 consensus reports of the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (UNGGE).

National Developments

Phishing attacks in India are on the rise

On October 20, Microsoft reported that consumers in India experienced a relatively high scam encounter rate of 69 percent between January 2020 to May 2021. The report observed that seven out of 10 consumers in India were targeted in the last 12 months. Cyber criminals are now using innovative ways to defraud innocent users into opening a malicious email or clicking on a link, containing malware that can cost users their personal information, exposing them to financial losses.[1] Another report by Norton Labs on October 26 indicated that more than 17 million cyber safety threats were successfully blocked in India over the past quarter. Norton also blocked more than 12.3 million tech support URLs, which topped the list of phishing threats for 13 consecutive weeks between July and September.[2] Also, the global cyber security company Trend Micro reported on October 27 that around 40.9 billion email threats, malicious files and URLs were blocked in the first half of 2021 globally, and in India it had blocked a total number of 1,11,028 email spam, malicious URLs and malware. Tech support scams, which often arrive as a pop-up alert convincingly disguised using the names and branding of major tech companies, have become the top phishing threat to consumers.[3]

All these reports point towards vulnerabilities of Indian enterprises. According to official estimates, cyber-attacks increased by 500 per cent during the pandemic due to adoption of digitisation. India suffered a loss of around Rs 1.24 lakh crore in 2020 due to cyber-attacks. There was no major impact on big players but financial crime increased and there was a 150 per cent rise in ransomware attacks.[4] India is at the sixth place among140 countries most affected by ransomware.[5]

In a public interaction on October 26, the National Cyber Security Coordinator pointed out that India remains a target because of a large attack surface with 1.15 billion phones and more than 700 million Internet users. Investigations show that cyber criminals route their attacks through three-four different destinations and the last hop is generally from a country like the US, Netherlands and Germany which uphold democratic values, strong privacy

[1] Here's how to protect yourself from phishing attacks (indianexpress.com)
[2] https://www.firstpost.com/india/tech-support-scams-are-biggest-phishing-threat-to-consumers-says-norton-labs-report-10087211.html
[3] Over 1.72 cr cyber safety threats blocked in India: Report - The Statesman
[4] pant: Central body accountable for nation's cyber security missing: NCSC Pant | India News - Times of India (indiatimes.com)
[5] India 6th most affected country by ransomware, says Google | Business Standard News (business-standard.com)

laws and good relations with India. This makes the task difficult for Law Enforcement Authorities. Interestingly, more than 30 per cent of the cyberattacks were from the US. The NCSC said that the National Cyber Security Strategy is at the final stages of approval, that will seek to address growing cyberattacks from nation state actors and cyber criminals.

Change in telecom landscape with 5G trials and reforms

Amidst ongoing 5G trials, Airtel reported on October 5 that India's first rural 5G trial was a success by utilising the allocated mid-band trial spectrum in the 3500MHz band.[6] The trial also showcased that a globally inter-operable 3GPP standards-based 5G smartphone could connect to the test network and record over 100Mbps speeds at a distance of more than 10km from the site. The 5G site was powered by Ericsson's 3GPP-compliant 5G radio.

However, the ambiguity regarding the allotment of millimetre wave bands (26 GHZ and 28 GHZ) for 5G has raised concerns. On October 26, the Telecom Regulatory Authority of India (TRAI) has sought clarity from the telecom department around the possible inclusion of millimetre wave bands in the 5G auction, as these bands have not yet been included/notified in the National Frequency Allocation Plan (NFAP) which is the key national spectrum policy document. The millimetre Wave band is considered most suitable for 5G services and certain use cases. The pricing of 5G frequency spectrum will be decided based on the quantum of spectrum available and terms of sharing these airwaves among stakeholders, including satellite and telecom players. industry leaders need to study global best practices on spectrum management in the 'closely related' yet complex space and telecom sectors to evolve policy in this area. To enable readiness of the eco-system, telecom players have asked for the extension of the 5G trial by one year.

The report 'Digital reset - touching a billion Indians' launched by Deloitte along with CII on October 13, suggests that technological innovations with 5G will redefine the future of telecom in India, while amalgamation of telecommunications services with upcoming industries and tech enablers (IoT, 5G, and private networks) will reorient the sector from being a 'service provider to a service enabler'. 5G networks would be mostly business driven and private networks are expected to see a huge demand from enterprises in the near future, led by the requirement of security and high-speed connectivity.[7]

[6] Bharti Airtel, Ericsson conduct India's first rural 5G trial, Telecom News, ET Telecom (indiatimes.com)

[7] 5g networks: 5G to accelerate private networks spend to $12 billion by 2023: Juniper Research, IT News, ET CIO (indiatimes.com)

5G trials have also taken a boost from the telecom sector reforms. On October 6, the Department of Promotion of Industry and Internal Trade (DPIIT) formally issued the press note for 100% FDI in the telecom sector, under the automatic route of approval, affecting all telecom services including Telecom Infrastructure Providers. The press note has invoked the 2020 mandate that restricts investment by neighbouring countries sharing borders with India. Also, it has clarified that the licensing conditions on security shall be observed by investors and licensee/entities providing telecom services.[8]

On October 14, the government finalised 31 global and local companies for the production linked-incentive (PLI) scheme. This will boost domestic manufacturing in telecom and networking products and accelerate domestic research & development of telecom equipment and applications for the 5G networks.[9]

Accreditation of labs for telecom equipment testing

To ensure security of networks, supply chain integrity needs to be assured by deploying trusted equipment that need to be tested and certified. The infrastructure required for the process is currently limited within the government. To scale up, private companies are also being accredited for the mandatory telecom equipment testing and certification. On October 13, four product testing laboratories of TUV Rheinland, located in India, have been designated as Conformity Assessment Bodies (CABs) by the Ministry of Communication's Telecommunication Engineering Centre (TEC) to conduct testing of telecom products under the Mandatory Testing and Certification of Telecom Equipment (MTCTE) Regulations. The certification would be effective from July 2022.[10]

Space technology to enhance communication reach

Communication is expected to take a leap forward with the launch of the Indian Space Association (ISpA), a grouping of space and satellite companies, by the Prime Minister on October 11. Partnership of the private sector with the Indian Space Research Organisation (ISRO) will help make India a vital player

[8] https://www.livemint.com/industry/telecom/govt-notifies-100-fdi-in-telecom-sector-through-automatic-route-with-riders-11633533325443.html
[9] https://www.financialexpress.com/industry/govt-launches-pli-scheme-for-telecommunication-manufacturing/2350048/
[10] telecom news: TUV Rheinland's Indian labs receive TEC accreditation for telecom equipment testing, Telecom News, ET Telecom (indiatimes.com)

in the global supply chain. Space and telecom combined could also enhance communication reach.[11]

On October 11, OneWeb partnered with the New Space India Limited (NSIL), the commercial arm of Indian Space Research Organisation (ISRO), to use Indian-built PSLV (Polar Satellite Launch Vehicle) and the heavier GSLV-MkIII (Geosynchronous Satellite Launch Vehicle) as potential platforms to launch its satellites in India. By late 2022, OneWeb is expected to offer its high-speed, low latency connectivity services in India. OneWeb is building its initial constellation of 648 LEO satellites and has already put 322 satellites into orbit.[12]

An independent panel to probe the Pegasus controversy

In a significant judgment passed on October 27, the Supreme Court appointed an expert technical committee overseen by a former Supreme Court judge, Justice R.V. Raveendran, to examine allegations of the possible unlawful use of Pegasus spyware. The Israeli origin Pegasus is a highly-advanced spyware that can allegedly steal passwords, contacts, text messages, calendar information, as well as voice and video calls made through WhatsApp, and can even track live location. The Supreme Court deliberated at length on the right to privacy and stressed that the mere invocation of national security by the State does not prevent the Court in protecting citizens from breaches in their privacy. The Court highlighted the importance of appointing an independent committee of experts who are free from bias.[13]

Justice Raveendran would be assisted by Alok Joshi, former Chairman of the NTRO and Sundeep Oberoi, Chairman, Sub Committee in the International Organisation of Standardisation. The three members of the technical committee are Naveen Kumar Chaudhary, Prabaharan P and Ashwin Anil Gumaste, all renowned professors on the subject. The Committee has been requested to prepare the report after a thorough inquiry and place it before the Court expeditiously. The Court would reconvene after eight weeks to discuss the findings.[14] The report of the committee and, ultimately, the directions and remedial measures provided by the Supreme Court, would be significant.[15]

[11] space sector: PM offers ISRO Tech, resources for private players to take to space, Telecom News, ET Telecom (indiatimes.com)
[12] oneweb: Bharti's OneWeb partners ISRO's commercial arm to use PSLV, GSLV for satellite launch in India, Telecom News, ET Telecom (indiatimes.com)
[13] Pegasus: Members and terms of reference of the Committee appointed by the Supreme Court (barandbench.com)
[14] Supreme Court Order on the WRIT PETITION (CRL.) NO. 314 OF 2021 and others of October 27, 2021
[15] Apar Gupta writes: How do we read the Supreme Court's Pegasus order (indianexpress.com)

5-year strategic Perspective plan on technology rollout

On October 19, it was reported that the government is looking at rolling out a five-year strategic perspective plan to make India a significant tech player, by partnering with the private sector in areas not just limited to commercial projects but for future technology developments like quantum computing, artificial intelligence, cybersecurity and semiconductors. The consultations to prepare a road map for India to emerge as a significant player in the technology space has been initiated.[16]

[16] https://cio.economictimes.indiatimes.com/news/government-policy/govt-to-roll-out-5-year-strategic-perspective-plan-to-make-india-big-tech-player-rajeev-chandrasekhar/87149685

International Developments

Ransomware attacks hit global cyber space

On October 25, Microsoft reported that the Russia-backed Nobelium threat group behind last year's Solar Winds hack is again active targeting the global IT supply chain, only months after President Joe Biden imposed sanctions on a Russian agency in response to a series of sophisticated spy operations. The company noted that more than 600 organisations had been the targeted by nation state actors. Nobelium is the hacking division of the Russian Foreign Intelligence Service (SVR), also tracked as APT29, Cozy Bear, and The Dukes. U.S. officials confirmed that the operation, which they consider as routine spying, was underway.[17]

On October 14, US agencies issued a joint advisory that its Water and Wastewater Systems (WWS) Sector facilities have been breached multiple times in ransomware attacks during the last two years. The alert issued jointly by the FBI, CISA and the NSA, highlighted the risks related to data, ransomware, network segmentation and shares information on the tactics, techniques and procedures (TTPs) used by threat actors to compromise IT and OT systems of water facilities and other critical networks. It also provides recommendations on how organisations can prevent, detect, and respond to cyber threats regarding such attacks.

The U.S. classifies water and wastewater systems as national critical functions, and their disruption or corruption would "have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof". The advisory revealed that multiple ransomware strains were used to encrypt water treatment facilities' systems.[18]

Similar advisories were initiated by many other developed economies against ransomware attacks which posed immediate danger to national security and economy. It was reported on October 11 that the head of the UK's National Cyber Security Centre (NCSC) has assessed that cybercriminals based in Russia were responsible for most of the "devastating" ransomware attacks against the UK.[19]

[17] https://indianexpress.com/article/world/russia-challenges-biden-again-with-broad-cybersurveillance-operation-7589666/
[18] https://www.securityweek.com/ransomware-hit-scada-systems-3-water-facilities-us
[19] https://www-bbc-co-uk.cdn.ampproject.org/c/s/www.bbc.co.uk/news/uk-58877433.amp

Iran Blames Cyberattack as Fuel Supply Hit

Iranian authorities on October 26 blamed a mysterious cyber-attack for unprecedented disruption to the country's fuel distribution network. The Supreme National Security Council confirmed the cyber-attack against the petrol distribution computer system. Details of the attack and its source are under investigation. The disruption had an impact because it blocked the IT system that allows Iranians to fill their tanks for free or at subsidised prices with a digital card issued by the authorities.[20] The disruptions came ahead of the second anniversary of an increase in fuel prices in November 2019 which led to widespread street protests in which hundreds were reported to have been killed by security forces.[21]

Israeli Hospital Targeted in Ransomware Attack

Earlier, on October 13, an Israeli hospital was targeted by a ransomware attack, with the state's cyber directorate calling it the first such attack on a hospital in the country.[22] Iran and Israel regularly accuse each other of cyber-attacks, since the Stuxnet attack that infected Iran's nuclear programme, causing a series of breakdowns in centrifuges used to enrich uranium, believed to be engineered by the US and Israel.

North Korean hackers target IT supply chain

On October 26, Kaspersky reported that the North Korea-linked state-sponsored hacking group Lazarus has started to target the IT supply chain in recent attacks. The Lazarus group compromised a legitimate South Korean security software to build an infection chain and deploy their malicious payload, for cyber-espionage purposes against South Korean think-tanks and an IT asset monitoring solution vendor.[23] Active since 2009 and also referred to as Hidden Cobra, Lazarus is believed to have orchestrated multiple high-profile attacks in 2020.

Microsoft Folds LinkedIn Social-Media Service in China

On October 14, LinkedIn announced its decision to quit from China, due to challenging operating environment and greater compliance requirements. LinkedIn had been operating there since 2014 and its decision to quit comes at a time when China's Communist Party has accelerated regulatory controls over

[20] https://www.securityweek.com/iran-blames-cyberattack-fuel-supply-hit
[21] https://www.business-standard.com/article/international/possible-cyberattack-hits-iranian-gas-stations-across-nation-121102601080_1.html
[22] https://www.securityweek.com/israeli-hospital-targeted-ransomware-attack
[23] APT trends report Q3 2021 | Securelist

its largest tech companies and private enterprises. LinkedIn will continue to provide a stripped-down version of its application to help China's job market.

In China, Twitter and Facebook platforms have been blocked since 2009 and Google left in 2010 after declining to censor results on its search engine. The chat messenger app Signal and audio discussion app Clubhouse were also blocked this year.[24] In May, Microsoft was the only foreign firm among 105 apps called out by China's internet regulator for "improper data collection," with both LinkedIn and Bing named on the list.

Whistle-blower exposes bias in Facebook algorithm

On October 5, Former Facebook employee-turned-whistleblower Frances Haugen testified to the US Congress, exposing internal documents that showed bias in the company's products affecting mental-health and political discourse and its inability/reluctance to prevent hate and fake messages. The leaked papers show how algorithms designed for maximising time spent on the platform ended up recommending hateful, inciteful and gory content or make Instagram a toxic platform for teenagers. According to her, "Facebook prioritised profit over consumer safety".[25] Her disclosures also included internal reports on hate speech and misinformation in India. She alleged that "much of it was intensified by its own recommendation on the algorithms".

Facebook took steps to dampen the spread of misinformation in users' feeds by a few tools designed for the purpose. These included a tool called "Sparing Sharing," which targeted "hyperposters," or accounts that post very frequently or another tool, called "Informed Engagement," that reduced the reach of posts that people were more likely to share if they hadn't read them. However, inefficient employment of these tools was coupled with skewed allotment of Facebook's global budget for classifying misinformation. It is reported that 87% of Facebook fund is allocated for the United States which accounts for only 10% of its total user base, while just 13% of its budget were allotted for remaining countries, including India, with greater market share.

Facebook Rebrands Itself Meta

On October 28, Facebook rebranded itself as 'Meta'. The change was accompanied by a new corporate logo designed like an infinity-shaped symbol. Facebook and its other apps, such as Instagram and WhatsApp, will remain under the Meta umbrella. The move signifies its plans to refocus on the new concept 'Metaverse' that melds online, virtual and augmented worlds for

[24] Microsoft Folds LinkedIn Social-Media Service in China - WSJ
[25] Facebook Whistleblower's Testimony Builds Momentum for Tougher Tech Laws - WSJ

consumers to traverse seamlessly, which would be the next major social platform. Renaming Facebook may help distance the company from the social networking controversies it is facing, including demand by its own Oversight Board for more transparency, a record fine of £50million by the UK competition watchdog, and roll back of its cryptocurrency project, besides the latest allegations by a whistle blower.[26]

Former U.S. President launches his own social media app

On October 21, former U.S. President Donald Trump announced the launch of a new social media platform 'TRUTH Social' through the merger of the Trump Media and Technology Group and a special purpose acquisition company. 'Truth Social' has been created as part of an effort by Mr. Trump to stand up to Big Tech, after he was banned by Facebook and Twitter in the wake of the January 6 assault on the U.S. Capitol.

TRUTH Social plans a nationwide rollout in the first quarter of 2022, while its future plans include launch of a subscription streaming service that would feature entertainment programming, news and podcasts. It is expected that with a subscriber base of 2 million, the platform could generate $240 million a year in revenue with minimal content expense.[27]

Global Chip Shortage 'Is Far from Over'

It was expected that the supply chain of semiconductor chips will bounce back this year with the decline of Coronavirus infections. However, the $464 billion semiconductor industry has been unable to keep pace, leading to lost revenue across the board. It was reported on October 28 by the Wall Street Journal that the global semiconductor shortage is worsening, with wait times lengthening, buyers hoarding products and the chip shortages seems to be spreading beyond the car makers and home appliance manufacturers to producers of other products, including smartphones and medical devices. The smartphone industry will grow by half the initial forecast, because the chip-making process is under duress. Basic building-block materials such as substrates are in short supply. Mishaps from bad weather and fires have interrupted wafer production. Global shipping constraints have added to disruptions and delays. The world's largest contract chip maker, TSMC, has boosted auto-chip production by 60% this year, yet car makers continue to struggle. Even companies like Apple Inc.

[26] apnews.com
[27] WSJ October 24, 2021

and Tesla Inc. have noted challenges in meeting customer demand, due to lack of critical components.[28]

US State Department Plans New Cybersecurity Office

On October 26, the US State Department announced plans to create a new bureau of cyberspace and digital policy as part of an overhaul to confront global cybersecurity challenges such as ransomware attacks. The restructuring will also include creation of a separate position of special envoy for critical and emerging technology. The move follows a Presidential executive order in May, aimed at improving US cybersecurity defences in the wake of the ransomware attack that forced the shutdown of a major US petroleum pipeline. A Senate report issued in August had criticised several federal agencies for weak cybersecurity practices.[29]

European Parliament calls for cybersecurity capacity

Global cyberattacks have harmonised responses across major economic powers. On October 7, the European Parliament called on the European Commission and EU member states to allot money, resources, and better coordination, dedicated to cyber defence. It observed that the EU Cybersecurity Agency (ENISA), unlike US agencies, lacked funds, resources and experts. Earlier on June 23, the European Commission had proposed building a joint cyber unit to tackle the rising number of serious cyber incidents impacting public services, businesses and citizens across the EU. The joint cyber unit would act as a platform bringing together resources and expertise from the different cyber communities in the EU and its member states to effectively prevent, deter and respond to mass cyber incidents.[30]

[28] https://www.wsj.com/articles/apple-tesla-to-take-hit-from-chip-shortage-a-sign-of-problems-intensity-11627474416?mod=article_inline
[29] https://www.bollyinside.com/news/us-state-department-plans-new-cybersecurity-office
[30] https://www.wsj.com/articles/intel-plans-investment-of-up-to-95-billion-in-european-chip-making-amid-u-s-expansion-11631027400?mod=itp_wsj&mod=djemITP_h

International Cooperation

International Anti-Ransomware Summit

On October 13, the US administration held a meeting with representatives from 30 countries, including NATO allies, EU and G7 partners, to discuss methods to combat ransomware. Russia was not invited. The meeting was aimed at accelerating international cooperation in combating cybercrime, improving law enforcement collaboration, stemming the illicit use of cryptocurrency, and engaging on these issues diplomatically. Other topics reportedly discussed included 5G technology, supply chain attacks, quantum computing, and artificial intelligence. The meeting underscored the transnational nature of the ransomware threat. India played a leading role during the meeting, along with the UK, Germany and Australia, to organise specific thematic discussions. "The meeting on tackling ransomware is part of the Joe Biden administration's four-part strategy to harmonise responses to ransomware attacks".[31]

Cybersecurity resolution at the UN General Assembly

On October 19, it was reported that Russia and the US have developed a UN General Assembly draft resolution on cybersecurity based on the 2021 consensus reports of the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (UNGGE). The document noted that "it is in the interest of all States to promote the use of information and communications technologies (ICTs) for peaceful purposes and to prevent conflicts arising from the use of ICTs." The resolutions might be put up for voting in December 2021.[32] The report followed a thematic debate held at the UN First Committee (Disarmament and International Security), on October 18, to propose a new programme of action for struggle against Threats to Cybersecurity.[33]

Fourth India-France Bilateral Cyber Dialogue

On October 13, the Fourth India-France Bilateral Cyber Dialogue was held in virtual mode. The Cyber Dialogue discussed various aspects of existing bilateral cooperation in cyberspace, exchanged views on the latest developments on cyber issues at bilateral, regional and multilateral fora and explored initiatives to further deepen cyber cooperation. The delegations deliberated on a wide

[31] https://huntdailynews.in/cybersecurity-india-takes-lead-on-joe-bidens-initiative-against-ransomware-world-news/
[32] https://tass.com/economy/1351085
[33] Delegates Propose New Programme of Action for Struggle against Threats to Cybersecurity, in First Committee Thematic Debate | Meetings Coverage and Press Releases (un.org)

range of topics of mutual importance and agreed to work closely with each other in the areas of cybersecurity, cybercrime and capacity building.[34]

[34] https://www.mea.gov.in/press-releases.htm?dtl/34405/Fourth_IndiaFrance_Bilateral_Cyber_Dialogue

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

www.delhipolicygroup.org