Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

JUNE 2021

Volume II, Issue 6 | June 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 6
June 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 6
June 2021

Contents

Abstract

The month of June has seen a number of cyber espionage attacks by intelligence agencies of China and Pakistan on India's sensitive and critical systems. In an effort to address the exponential increase of cyber fraud and to provide a secure digital payments eco-system to its citizens, the Indian Government has operationalised a national Helpline number and its Reporting Platform, hosted by the Indian Cyber Crime Coordination Centre (I4C). The standoff between the government and social media platforms over the implementation of the Information Technology (IT) Rules 2021 continued unabated. Speaking at an event, India's External Affairs minister underlined that a meaningful debate on the responsibility and accountability of influential big tech/social media companies vis a vis privacy and freedom of expression concerns is essential for a resolution of this impasse. Trials of fifth-generation (5G) communications got underway in June, with the active participation of major telecommunications service providers (TSP) and approved equipment vendors.

On the international front, the threats of disruptive and destructive cyberattacks, including cyber espionage, and cryptocurrency driven ransomware, were on the agenda of summit meetings held in June. World leaders will need to shape a global framework to restrain state-proxies from attacking the critical cyber infrastructure of geo-political adversaries.

Reports of Chinese cyber espionage on high value entities in the US, including the telecommunications firm Verizon, the New York subway system and California's largest water agency highlighted supply chain vulnerabilities.

To thwart attacks from adversaries, the European Commission has proposed a Joint Cyber Unit, to be launched by 2022, to serve as a hub for threat intelligence and as a first-responder to cyberattacks. While the new unit will cover both national security and corporate concerns, NATO will focus on military and diplomatic interests.

In Latin America, El Salvador became the first country in the world to grant legal tender status to Bitcoin, even as several countries, including China, are trying to curb the menace of crypto currency being used for criminal activities.

A report titled 'Cyber capabilities and national power: a net assessment', that assessed the cyber capabilities of 15 countries in 7 categories, was released by the International Institute for Strategic Studies (IISS) on June 28.

On May 28, the UN Group of Governmental Experts (UNGGE 2019-21) on "Advancing responsible State behaviour in cyberspace in the context of international security" adopted a consensus report that reaffirmed that international law and the UN Charter applies in its entirety to cyberspace. It also endorsed 11 norms of state behaviour with greater clarity. The UNGGE report complemented the broader report by the Open-Ended Working Group (UN-OEWG) on cyber security, released on March 12, 2021.

National Developments

Threat scenario in Indian Cyber Space

It was reported on June 10 that a Pakistani cyber espionage group operated illegal call exchanges that switch Voice over Internet Protocol (VoIP) calls to normal Indian mobile calls to steal data from Indian military personnel, defence contractors and important dignitaries.[1] Thirty-two SIM box devices with 960 SIM cards each were seized from the group. The operation was exposed by the Military Intelligence wing of the Army's Southern Command.[2]

Another report on June 17 indicated that a Chinese espionage group, Red Foxtrot, had targeted aerospace, defence, government, telecommunications, mining, and research organisations in India, among other countries, since 2014. The group is said to have linkages to the People's Liberation Army (PLA) intelligence Unit 69010, as part of the second Technical Reconnaissance Bureau (TRB) within China's Strategic Support Force (SSF). A previous report by Recorded Future had suggested that another Chinese malign group, RedEcho, was targeting India's critical infrastructure in the power and port sectors. The government of India clarified on June 13 that adequate security measures are in place and there has been no compromise of email systems maintained by the National Informatics Centre (NIC), contrary to some media reports.[3]

National Helpline for Cyber Fraud

Social distancing measures in India have accelerated the use of digital payment services over the past year. However, the increased use of financial services serves as a potential attack vector for cybercriminals. According to a report released on June 17, about 38% of Indian youth who prefer on line transactions have faced cyber fraud, including phishing attacks, QR code scams and card scams.[4]

In an effort to provide a safe and secure digital payments eco-system, the Indian Government has operationalised a national Helpline number 155260 and its Reporting Platform, hosted by the Indian Cyber Crime Coordination Centre (I4C), on June 17. The Citizen Financial Cyber Fraud Reporting and Management System has been developed in-house to integrate law

[1] Suspected Pakistani spies use catfishing, stealthy hacking tools to target Indian defense sector (cyberscoop.com)
[2] https://telecom.economictimes.indiatimes.com/news/illegal-telephone-exchange-used-for-spying-unearthed-in-bluru/83394271
[3] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1726821
[4] https://ciso.economictimes.indiatimes.com/news/youth-most-vulnerable-to-upi-scams-phishing-attack-report/83594370

enforcement agencies, banks and Financial Intermediaries, for sharing online fraud-related information and initiate near real time response. The National Cybercrime Reporting Portal (https://cybercrime.gov.in/) has been linked to this help line.[5]

Continuing standoff over IT Rules 2021

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 are being challenged from several quarters, even as the government remains firm on their implementation. While the US-India Strategic Partnership Forum (USISPF) has sought clarity on some contentious provisions, global technology companies and industry bodies are seeking removal of the clause that imposes personal criminal liability on the chief compliance officer of these intermediaries.

At the United Nations Office in Geneva, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association; and the Special Rapporteur on the right to privacy, issued a Joint Communication on June 11 calling for a review of India's IT Rules, 2021 contending that they do not conform with international human rights norms. The Permanent Mission of India in Geneva responded to these concerns and clarified that the due process of law has been followed for framing the rules.[6]

The new IT rules are also facing legal challenges, with WhatsApp challenging the mandate that requires it to trace the first originator of a message. Google, on the other hand, has filed a petition in the Delhi High Court arguing that its search engine was wrongly categorised as a significant social media intermediary. On June 23, the Madras High Court issued a notice to the Union Government based on a petition by the Digital News Publishers Association challenging the new IT rules.[7] Separately, the Delhi High Court has scheduled a hearing on July 9 for petitions filed by several media platforms, including the Foundation for Independent Journalism, who have challenged the constitutional validity of the new IT Rules that seek to regulate digital news media.[8]

The standoff between the government and Twitter also continues to persist. This was further aggravated on June 25, when Twitter denied the Union IT

[5] https://pib.gov.in/PressReleasePage.aspx?PRID=1727990
[6] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1728738
[7] Madras HC issues notice to Centre on petition from Digital News Publishers Association challenging IT rules - The Economic Times (indiatimes.com)
[8] Delhi HC seeks Centre's response to portal's plea - The Hindu

Minister access to his own account briefly, citing a violation of a US copyright law. Earlier, on June 15, the government had withdrawn the coveted "safe harbour" immunity to Twitter, granted under Section 79 of the IT Act.

While it is generally acknowledged that the big tech companies are 'forces of progress' facilitating freedom of expression, External Affairs Minister Dr. S. Jaishankar has underlined that there needs to be a vigorous debate on the responsibility and accountability of these platforms as 'non-state players' who enjoy huge power and influence on the society. Healthy outcomes from such debates should resolve the issue of the IT Rules 2021 holistically.[9] A standard operating procedure (SOPs) should also be evolved to ensure that due process of law is adopted.

Strengthening Communications Infrastructure

Data communications networks, as part of a secure cyber eco system, are essential for economic growth and development. In order to increase broadband penetration in rural and remote areas, the Prime Minister's WiFi Access Network Interface (PM-Wani) was launched in December 2020. The PM-Wani architecture will provide high-speed unlimited internet to the 500 million users in India who otherwise do not have data access. On June 6, it was announced that the first startup company, incubated in IIT-Delhi, is planning to deploy 100,000 public WiFi hotspots in 2021. Meanwhile, the Central government is also targeting the setting up of 2 million public WiFi access points by the end of 2021.[10]

Notwithstanding these efforts, India still has nearly 300 million 2G feature phone users, for whom a basic 4G smartphone remains beyond reach. A stark digital divide has been witnessed during the Covid-19 pandemic. The situation is likely to improve with the manufacture of global and domestic brand mobile phones under India's 'Make in India' program. In addition, on June 24, Reliance Jio announced the launch of an entry-level 4G affordable smartphone, jointly developed by Jio Platforms and Google, that will debut on September 10.[11]

Innovations and trials for 5G and beyond

The trials of fifth-generation (5G) communications got underway in June, with active participation by major telecommunications service providers (TSP) and

[9] https://indianexpress.com/article/india/big-tech-companies-twitter-debate-s-jaishankar-7383138/

[10] https://www.business-standard.com/article/economy-policy/tremendous-potential-for-proliferation-of-wi-fi-hotspots-in-india-trai-121061801616_1.html

[11] https://telecom.economictimes.indiatimes.com/news/jiophone-next-smartphone-developed-by-google-and-jio-to-be-available-on-sept-10-ambani/83806319

approved equipment vendors under the framework for the national security directive for the telecom sector. These TSPs are also making efforts to innovate software based open radio access network (O-RAN) solutions, to handle network functions. While cost reduction is the key advantage, O-RAN helps to bring agility to networks and provide flexibility to expand.

On June 21, Bharti Airtel and the Tata Group announced a strategic partnership to deploy O-RAN based radio and indigenous core technology, aligned to global 5G standards. Airtel plans to conduct trials and pilot successful solutions as part of its 5G rollout plans in January 2022.[12] Earlier, Reliance Jio had announced the deployment of its own indigenous equipment and technology, along with a partnership with Intel to "co-innovate" on 5G radio-access network (RAN), while fielding its 5G trial network. Both operators have claimed a throughput of over 1 Gbps, during the trials with their respective technologies.[13]

In spite of India being the second-largest telecom market, one area of concern has been the lack of development of Indian 5G standards. In 2020, the sole indigenous 5Gi standard, was approved by the International Telecommunications Union (ITU). Its main feature, Low Mobility Large Cell (LMLC), helps enhance the range of a mobile base station that would enable cost-effective expansion of 5G coverage in rural and remote areas. However, TSPs are hesitant to adopt 5Gi on grounds of interoperability and increases in deployment cost, as 5Gi has not yet been adopted globally as part of the 3GPP standard.

Having lagged behind on 5G, India has initiated R&D around 6G in right earnest. On June 22, India's telecom standards agency, the Telecom Standards Development Society (TSDSI), has submitted a vision document on 6G broadband technology to the ITU-Radiocommunications Sector (ITU-R). The strategy involves steering research to develop multiple radio access technologies and engagement with global standards bodies for harmonisation of efforts to ensure interoperability.[14]

[12] https://telecom.economictimes.indiatimes.com/news/airtel-partners-tata-group-to-deploy-indigenous-open-ran-5g-technology-in-india/83714108

[13] https://telecom.economictimes.indiatimes.com/news/jio-made-in-india-5g-tech-globally-competitive-ready-to-quickly-upgrade-networks-to-5g-ambani/83806821

[14] https://government.economictimes.indiatimes.com/news/technology/india-telecom-standards-body-submits-6g-vision-doc-to-itu/83802623

State of Cryptocurrency in India

The cryptocurrency industry, as part of over 200 blockchain startups in India, has welcomed the lifting of the ban on banks to deal in virtual currencies (VCs), announced by the RBI on May 31.[15] According to a report by the industry association IndiaTech.org, Indian users currently hold crypto assets worth more than $1.5 Bn. and their daily trades in crypto are worth $350-500 Mn.[16] There is thus a growing need for regulatory clarity to ensure innovations, while preventing crypto currency from becoming the currency for ransomware, cyber-extortion and impersonation. It is expected that the proposed legislation titled "The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021", will help make a significant breakthrough in this regard.[17]

[15] RBI issues clarification on use of bank accounts for cryptocurrency transactions (yourstory.com)
[16] https://inc42.com/buzz/crypto-exchanges-coming-together-to-lobby-for-regulation/
[17] Crypto exchange: Top crypto exchanges plan multi-pronged push for regulation - The Economic Times (indiatimes.com)

International Developments

Global Cyber Attacks take political centre stage

Attention from world leaders in multilateral summits held in June underscores the seriousness of threats of disruptive and destructive cyberattacks including ransomware, increasingly being perpetrated by state sponsored adversaries.

The Group of Seven (G7) meeting on June 12, the NATO summit on June 14, and the US-Russia summit on June 16, all called for curbs on state sponsored criminal groups working as proxies for military and intelligence organisations. In their Carbis Bay communique, the G7 announced their intention to work together to tackle ransomware groups. Efforts were made during the US-Russia summit to establish some "guardrails" that would make cyber-attacks on identified critical infrastructure off limits in peacetime and liable to suitable retaliation if they occur. An extradition process on a reciprocal basis to bring cybercriminals to justice was also discussed. Characteristically, allegations and counter allegations were made by both sides without much result. Among the outcomes of the US-Russia summit was an agreement to begin "consultations" on cyber-related issues.[18]

At the Moscow Conference on International Security held on June 24, the Russian Security Council Secretary Nikolai Patrushev alleged that a significant number of over 120,000 cyberattacks on Russia's "critical infrastructure" in 2020 had originated in the US, Germany and the Netherlands. He noted that while Russia is often "groundlessly accused of carrying out cyber-attacks against Western states", the NATO alliance has officially declared cyberspace as a military domain. He called for active cooperation at the UN and in other multilateral organisations for achieving strategic stability.[19]

India's National Security Advisor, Ajit Doval, held a meeting with his Russian counterpart on June 24, on the sidelines of the Shanghai Cooperation Organisation (SCO) NSAs meeting in Dushanbe, Tajikistan, with cyber-security among other strategic issues on the agenda.[20] Further, addressing a UNSC debate virtually on June 29, India's Foreign Secretary raised concerns about

[18] Summit Over, Putin and Biden Cite Gains, but Tensions Are Clear - The New York Times (nytimes.com)

[19] 'Over 120K cyber attacks carried out in 2020 on on Russian infrastructure', IT Security News, ET CISO (indiatimes.com)

[20] https://www.hindustantimes.com/india-news/russian-nsa-patrushev-briefs-doval-about-biden-putin-summit-101624593260744.html

cross border state-sponsored cyber-attacks, but without naming China or Pakistan.[21]

Critical entities face Chinese cyber espionage campaign

In yet another instance of a supply chain cyber-attack reported on June 14, dozens of high-value US entities, including the telecommunications firm Verizon, the New York subway system and California's largest water agency, were targeted by suspected Chinese hackers by breaching Pulse Secure, which is deployed for secure remote access to the internet. Though the extent of extraction of sensitive data for cyber espionage was not made public, the ease with which hackers gained footholds in critical entities should worry security professionals across the globe. Chinese hackers are also alleged to be exploiting zero-day vulnerabilities of different western-made antivirus products, procured locally, to target western enterprises. The Chinese government has denied involvement in any such campaign.[22]

European Union forms Joint Cyber Unit

Amidst mounting digital security threats, said to be originating mostly from China and Russia, the European Commission has proposed to launch a Joint Cyber Unit by 2022, to serve as a hub for threat intelligence and as a first-responder to cyberattacks. Under a detailed plan outlined on June 23, the Unit will establish rapid reaction teams to provide swift assistance to countries under attack. The unit also will serve as a platform for law enforcement, diplomatic communities, intelligence services and private-sector companies across the bloc to share resources and expertise on cyberthreats. The Joint Cyber Unit's mission overlaps in part with that of NATO. The new unit will cover both national security and corporate concerns, while NATO focuses on military and diplomatic interests.[23]

US seizes internet domains in Iran

More than 30 web domains linked to the Iranian regime were seized by U.S. agencies on June 22. The seized sites include government-run PressTV as well as social media channels affiliated with Iran-backed militias in Iraq. The seizures come in the midst of negotiations over Tehran's nuclear program and the election of a new Iranian President. The domains were seized in

[21] https://www.indiatoday.in/india/story/un-security-council-india-cyber-attacks-warfare-pakistan-china-1820899-2021-06-29
[22] Critical entities targeted in suspected Chinese cyber spying (apnews.com)
[23] EU to form united front to battle Chinese and Russian cyberthreats - Nikkei Asia

coordination with the U.S. Department of Commerce's Bureau of Industry and Security, which de facto controls the internet.[24]

Global collaboration against cyber criminals

A press briefing on June 8 revealed that a global sting operation dubbed "Operation Trojan Shield," which covertly monitored the encrypted communications service Anom, had been run secretly by the FBI. The platform was adopted by more than 12,000 alleged members of international criminal organisations across more than 100 countries to communicate securely. Anom applications were installed for covert communications on specially designed smartphones to provide security and anonymity.

More than 800 arrests of suspected members of these criminal networks were made in 16 countries and large quantities of drugs, firearms and currencies were seized. The globally coordinated campaign involved more than 9,000 law-enforcement offices. The FBI campaign highlighted the need to monitor and intercept encrypted communications for law enforcement, amid ongoing debates to balance security and privacy on technology platforms.[25]

US revokes ban on Chinese platforms

On June 9, an executive order by the US President revoked the ban on Chinese social media apps TikTok, WeChat and several payment platforms. The EO mandated the Commerce Department to carry out a broad review of apps controlled by foreign adversaries to collect sensitive personal data that could be used to support military or intelligence activities posing a security threat to the US, and to make recommendations within 120 days to protect US data acquired or accessible by companies controlled by foreign adversaries.[26]

There are, however, mixed signals from the Biden administration. Another executive order of June 3 had extended a ban on a total of 59 Chinese companies, with military links or in the surveillance technology sector, from receiving American investment. These included state-owned Aviation Industry Corporation of China and two financing affiliates of Huawei Technologies Co.[27]

[24] U.S. Seizes Internet Domains Tied to Iran's Government - WSJ
[25] The FBI Secretly Ran the Anom Messaging Platform, Yielding Hundreds of Arrests in Global Sting - WSJ
[26] China says US revoking of China apps ban a 'positive step' (apnews.com)
[27] Biden Expands Blacklist of Chinese Companies Banned From U.S. Investment - WSJ

Bitcoin adopted as legal currency

While the majority of the global community, including China, has shunned crypto currency in favour of Central Bank Digital Currency (CBDC) as Legal Tender, El Salvador has become the first country in the world to grant legal tender status to Bitcoin. The Central American Nation's Bitcoin law was approved in the legislative assembly on June 9 by a "supermajority". Its adoption implies that the exchange rate between Bitcoin and the US dollar will be freely established by the market. Prices and tax contributions may be expressed in Bitcoin. Exchanges in Bitcoin will not be subject to a capital gains tax, just like any legal tender. The move will have an impact globally and may complicate El Salvador's talks with the IMF for a $1 billion support program.[28]

In the meanwhile, the Chinese authorities intensified a crackdown on unregulated virtual currencies. On June 21, China's central bank ordered the country's largest banks and payment processors to curb cryptocurrency trading and related activities. Chinese police have recently arrested persons suspected of using cryptocurrencies for money laundering. Despite these efforts, China has remained a hotbed for cryptocurrency mining, with up to three-quarters of the world's production of Bitcoin. The public in China has also continued to trade Bitcoin and other digital currencies via peer-to-peer transactions that involve direct money transfers between accounts. The Chinese government is about to launch a national digital currency, controlled by the central bank, to counter cryptocurrencies.[29]

IISS report on cyber power ranking

A report titled 'Cyber capabilities and national power: a net assessment', released by the International Institute for Strategic Studies (IISS) on June 28, assessed the cyber capabilities of 15 countries in seven categories, including strategy and doctrine; cyber security and resilience; and offensive cyber capability.

The report placed the US in the first tier, for its world-leading strengths across "all" categories, while India along with Japan, Iran, Indonesia, Vietnam, Malaysia and North Korea have been placed in tier 3, meant for countries that have strengths or potential strengths in some of these categories but "significant weaknesses" in others. In the second tier, with world-leading strengths in "some" categories are: Australia, Canada, China, France, Israel, Russia and the United Kingdom. The report assessed that in advanced cyber

[28] El Salvador creates history: Becomes world's first country to adopt Bitcoin as legal currency - The Financial Express

[29] China Reconsiders Its Central Role in Bitcoin Mining - WSJ

technologies and their exploitation for economic and military power, the US is still ahead of China. However, because of its growing indigenous digital-industrial capacity, China is on a trajectory to join the US in the first tier.[30]

The study observed that India's offensive cyber capability is Pakistan-centric rather than focused on China. Despite the regional geo-strategic instability, India has made only "modest progress" in developing its policy and doctrine for cyberspace security. The country is active and visible in cyber diplomacy but has not been among the leaders on global norms. To move to tier 2, India needs to harness its "great digital-industrial potential and adopt a whole-of-society approach" to improve its cyber security.[31]

[30] New IISS Research Paper CYBER CAPABILITIES AND NATIONAL POWER: A Net Assessment

[31] India's offensive cyber capability more focused on Pakistan than China, UK think tank says (theprint.in)

International Cooperation

UNGGE Report 2019-2021 adopted

The final report of the UN Group of Governmental Experts (GGE) on "Advancing responsible State behaviour in cyberspace in the context of international security" was adopted unanimously on May 28, 2021. The report reaffirmed that international law and the Charter of the UN applies in its entirety to cyberspace and that international humanitarian law applies in the case of armed conflict. The consensus report by the 25-member group, including India, has developed additional layers of understanding to the 11 norms of state behaviour, which had been recommended by the 2015 GGE. For the first time, the report recognised the role of proxies to commit internationally wrongful acts using ICTs, and the responsibility of states to ensure that their territory is not used by non-state actors to commit such acts. It urged regional and sub-regional bodies to take the next steps to implement the report's recommendations. The UNGGE report complements the work of the broader Open Ended Working Group (UN-OEWG) on Cyber Security, which had submitted its report in March 2021.[32]

In spite of past inputs, the report continues to be a work in progress. Experts believe that there has not been much "value addition" to the understanding of the crucial relationship between state conduct in cyber space and international law. Also, the understanding of legal constraints that apply to damaging and disruptive offensive cyber operations below the threshold level of armed conflict has remained vague. The report, however, is a welcome step to encourage nations to adopt confidence building and cooperative measures required among members of the global community to achieve cyber peace and strategic stability.

India-Australia Cyber Cooperation

The Joint Working Group (JWG) on Cyber Security Cooperation between India and Australia met virtually on June 10, reaffirming their commitment to work together in the areas of digital economy, cyber security and emerging technologies. Both countries shared threat assessments, cyber strategies and information on legislation. The meeting was established under the 'Framework Arrangement on the Cyber and Cyber-enabled Critical Technology

[32] https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

Cooperation' between the two Quad member countries to implement their 2020-25 plan of action.[33]

[33] India-Australia reaffirms commitment to work together in areas of digital economy, cyber security (aninews.in)

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

www.delhipolicygroup.org