Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

MAY 2021

Volume II, Issue 5 | May 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 5
May 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 5
May 2021

Contents

Abstract i
National Developments 1
The Cyber Threat Scenario 1
Social Media vs. National Laws 1
5G Trials begin in India 3
Self-sufficiency in electronics manufacturing 3
Capability building in Quantum computing 4
International Developments 5
Vital US Oil pipeline experiences ransomware attack 5
SolarWinds hackers strike again with phishing attacks 6
Ransomware linkages to Crypto currencies 6
Belgian Government websites suffer DDOS attacks 7
North Korean Cyber threats are more immediate: US ODNI 7
Social Media vs. Government of Canada 8
Artificial Intelligence War 8
The US-China technology slugfest 9
International Cooperation 10
India-EU Leaders' Meeting 10
India-UK Virtual Summit 10

Abstract

The revelation this month of the hacking of the Indian carrier, Air India, that compromised the personal data of more than 4.5 million passengers, is disturbing. Personal data from several other Indian organisations has been stolen in recent months and placed on the dark web for sale. Such data breaches call for effective security and accountability measures.

Effective from May 26, social media platforms in India are required to comply with new IT Rules 2021 that codify provisions under national laws to enhance accountability, security and public order. Most social platforms have faltered in their compliance. Trust between them and the Indian government has been further shaken by public acrimony and resort to legal recourses.

The much-awaited 5G trials are set to begin in India with experimental 5G spectrum. Global and indigenous technology along with equipment identified by telecom service providers will be tried, to test Indian use cases. Chinese vendors have been excluded from the 5G trials.

A series of cyberattacks this month have exposed the regulatory laxities to secure US domestic networks. A major ransomware attack on a vital US oil pipeline, and phishing attacks on several email accounts by hackers earlier linked to the SolarWinds cyber espionage, come days before a meeting between Presidents Biden and Putin in Geneva.

The Covid-19 pandemic has also ushered in a global ransomware pandemic. Most criminal attacks on critical infrastructure or sale of personal/enterprise data on the dark web aim for extortion through crypto currencies. This has led some experts to suggest that the menace of ransomware attacks can be stopped by banning cryptocurrencies, or by imposing effective regulatory measures.

The United States and China are aggressively competing on every aspect of digital technology, and in all geographies. Both countries are trying to out-subsidise and out-innovate each other to retain a technological edge.

National Developments

The Cyber Threat Scenario

There have been a series of hacking incidents involving Indian firms in the recent past. 13TB data of nearly 1.8 million orders of Domino's India have been made public on the Dark Web. An Israeli security firm reported on May 18 that India has seen the greatest number of ransomware attack attempts per organisation since the beginning of the year.[1] Another report suggests that there is a steep 90-100% increase in account takeover (ATO) on the dark web. ATO refers to online identity theft where a cybercriminal accesses personal financial information to commit cybercrime or fraud.[2]

A massive data breach has compromised personal data, including passport information, of 4.5 million passengers of Air India, registered between August 26, 2011 and February 20, 2021. As revealed on May 21, the PSS Server of the multinational firm, SITA, that stored and processed personal information, was compromised at its Atlanta centre. The attack has also affected passengers of other airlines such as Malaysia Airlines, Finnair, Singapore Airlines, Lufthansa and Cathay Pacific.[3]

The attack raises concerns on security of data stored beyond national borders and accountability of third-party services and product providers. Since the operationalisation of the IT Act in 2000, there has hardly been any penalisation for data breaches. It is being suggested that better accountability and transparency be imposed by the Indian Computer Emergency Response Team (CERT-In). A holistic approach by regulators, supply chain partners and organisations handling end-user data is needed to enhance public security posture.[4]

Social Media vs. National Laws

During the month, social media platforms have been at odds with the Indian establishment. Multinational platforms dominate the Indian market with 530

[1] India facing 213 weekly ransomware attacks per organisation: Report, IT News, ET CIO (indiatimes.com)

[2] https://ciso.economictimes.indiatimes.com/news/identity-theft-via-e-commerce-ott-accounts-on-rise-study/82789597

[3] https://www.timesnownews.com/business-economy/companies/article/cyber-attack-air-india-servers-hacked-customers-credit-card-details-compromised/760146

[4] https://economictimes.indiatimes.com/tech/information-tech/air-india-bigbasket-dominos-why-no-action-against-data-breach-ask-cybersecurity-experts/articleshow/82943377.cms

million WhatsApp users, 448 million YouTube users, 410 million Facebook subscribers and 210 million Instagram clients, while 17.5 million account holders are on the microblogging platform Twitter. The only indigenous platform, Koo, has close to 6 million users. These platforms are classified as 'significant' social media intermediaries under the new IT Rules and guidelines of February 25, 2021.

The 'Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021', which became effective from May 26, require 'significant' social media intermediaries to enable traceability of the originator of information that undermines the sovereignty of India, security of the state, or public order. Other provisions include the appointing of a chief compliance officer, a nodal contact person, and a resident grievance officer. The IT Rules 2021 aim to make these platforms more accountable and responsible for the content hosted on their sites.

By the mandated cutoff date, only Koo had confirmed its compliance. Google and Facebook have both expressed their readiness to comply with the revised IT Rules.[5] WhatsApp has filed a legal complaint on May 25 in the Delhi High Court against the Rules, contending that the traceability provision is unconstitutional and against the fundamental right to privacy.[6] The Government has clarified in a press release that it recognises the right to privacy but social media platforms need to adhere to the laws of the land.[7] These platforms face the prospect of losing their safe harbour guarantee given to intermediaries under Section 79 of the IT Act.[8]

There has also been an acrimonious exchange of press releases on May 27 between Twitter and the Indian government over a "toolkit" that revealed distrust between the social media platforms and the Indian establishment over the new IT Rules.[9] On May 31, the Delhi High Court gave Twitter three weeks to show it is compliant with India's new IT rules, unless stayed by a court.[10]

[5] https://telecom.economictimes.indiatimes.com/news/google-facebook-say-ready-to-comply-with-revised-it-rules/82962460

[6] https://www.outlookindia.com/website/story/india-news-whatsapp-moves-delhi-hc-against-centres-new-it-rules/383612

[7] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1721915

[8] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1721915

[9] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1722252

[10] https://www.thehindu.com/news/national/twitter-has-to-comply-with-new-it-rules-for-digital-media-says-delhi-high-court/article34687483.ece

While WhatsApp has scrapped its May 15 deadline for users to accept its controversial privacy policy update and announced that not accepting the terms will not lead to deletion of accounts, it has not withdrawn these new privacy rules. Consequently, the Indian government, on May 18, has directed WhatsApp to rescind its new Privacy Policy 2021, and to respond within the next seven days.[11]

Interestingly, as reported on May 12, Germany has also banned Facebook from processing WhatsApp user data, because it views the messaging app's new terms of use as illegal and also amounting to an abuse of market dominance.[12] Germany adheres to the EU's General Data Protection Regulation (GDPR).

5G Trials begin in India

The much-awaited 5G trials in India are set to begin. On May 4, major telecom service providers (TSPs) got the go ahead for conducting trials of 5G technology in rural, urban and semi-urban settings.[13] These TSPs have tied up with original equipment manufacturers and technology providers of non-Chinese origin. The trials will be conducted on Indian use cases and indigenous technologies, including the International Telecommunication Union (ITU) recognised indigenous 5Gi technology, that facilitates much larger reach of 5G towers and radio networks.[14]

TSPs will be permitted to use their existing spectrum of 4G owned by them, along with experimental 5G spectrum allotted by the government on May 27, ie. "100, 800 and 10 units respectively in the mid band (3.5 GHZ), millimetre wave band (26 GHZ) and sub GHZ band (700 Mhz)". The trial would pave the way for inclusion of these spectrums in the revised National Frequency Allocation Plan (NFAP-2021). The duration of the trials, at present, is for a period of 6 months.[15]

Self-sufficiency in electronics manufacturing

India is the second-largest telecommunications market and with TSPs moving towards 5G technology, domestic manufacturing will play a pivotal role. With

[11] https://economictimes.indiatimes.com/tech/technology/breaking-govt-tells-whatsapp-to-withdraw-privacy-policy-serves-seven-day-notice/articleshow/82764158.cms?from=mdr

[12] https://ciso.economictimes.indiatimes.com/news/german-regulator-bans-facebook-from-processing-whatsapp-user-data/82570556

[13] https://content.pib.iostechtools.com/1715927/web.html

[14] https://content.pib.iostechtools.com/1715927/web.html

[15] https://telecom.economictimes.indiatimes.com/news/government-oks-13-applications-for-5g-trials-chinese-vendors-kept-out/82383855

production linked incentive schemes (PLI 2020) and the National Policy on Electronics 2019, India aspires to be a global hub for Electronics System Design and Manufacturing (ESDM) and to have $400 billion of electronics manufacturing by the year 2025.

As notified on May 4, a total of 19 companies have filed their applications under the PLI for IT Hardware. Production of Rs. 1.60 lakh crore ($22 billion) and Exports of Rs. 60 thousand crore ($8.3 billion) are expected over the next four years. These companies are expected to expand their manufacturing operations and eventually grow into national champions.[16]

It is also crucial that India becomes self-sufficient in manufacturing semiconductor chips. With various incentive-linked schemes, the country has a great opportunity to establish a full-fledged semiconductor fabrication (FAB) electronics manufacturing ecosystem in the country. The government has come out with an Expression of Interest (EOI) for setting up of semiconductor wafer or device fabrication facilities in India, or the acquisition of semiconductor FABs outside India. The last date for submissions was April 30, but the results have not yet been made public.[17]

Capability building in Quantum computing

Quantum computing has opened new frontiers in research in cyber-security, communications and computing, among others. The government of India had announced the National Mission on Quantum Technologies & Applications (NM-QTA) in Budget 2020, with a total allocation of ₹8000 crores ($1.1 billion) for five years. The initiatives are being steered by the Department of Science & Technology (DST).

The DST is working on the development for quantum computing in India, including post quantum cryptography and digital signatures, in collaboration with resources in India and abroad, to address future security needs.[18] The Indian Space Research Organisation (ISRO) is working to integrate satellite-based quantum communications with optical fibre based terrestrial communications, and on developing quantum atomic clocks, which will play a major part in the creation of a Navigation Indian Constellation (NAVIC) system. Besides, on May 27 a private company QNu Labs announced the launch of a Quantum Key Distribution system with a range beyond 100kms and a Quantum Random Number Generator Chip – Ikaria, that would provide

[16] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1715871

[17] https://www.meity.gov.in/esdm/FAB

[18] https://www.assocham.org/newsdetail.php?id=7525

enhanced security for IoT, Point of Sale (PoS) systems, mobile and security applications.[19]

International Developments

Vital US Oil pipeline experiences ransomware attack

A series of cyberattacks exposing vulnerabilities of US critical infrastructure and domestic networks are turning out to be embarrassing for the US. The Colonial Pipeline, spanning over 8,850 kilometres and delivering 45% of the fuel consumed by the U.S. East Coast, was hit by ransomware deployed by the criminal gang DarkSide, believed to be based in Eastern Europe. The attack was dubbed the "most disruptive digital ransom operation" and disrupted fuel delivery for six days from May 7. Operations resumed from May 12, reportedly after the company had paid a ransom of $4.4 million (75 Bitcoins in crypto currencies), possibly from its insurance cover of $15 million, in exchange for a decryption tool to unlock the systems that hackers had penetrated. Unlike other critical infrastructure like electric utilities, regulatory cyber security measures for oil pipelines were not being enforced, which is now being remedied.[20] The joint advisory of CISA and FBI has urged critical infrastructure owners and operators in the US to adopt regulatory measures, including implementing robust network segmentation between IT and OT networks, improved information sharing and ensuring backups.

On May 12, President Joe Biden signed an Executive Order (EO) for improving the nation's cybersecurity. The Secretary of Homeland Security, in consultation with the Attorney General, shall establish a Cyber Safety Review Board that would investigate major hacks along the lines of National Transportation Safety Board inquiries that are launched after plane crashes. The EO requires the National Institute of Standards and Technology (NIST) to set new guidelines for vendors that provide software to the government. The order mandates all federal agencies to encrypt both their stored and transmitted data.[21]

In a statement on May 18, the White House also detailed the cyber element of President Joe Biden's already proposed American Jobs Plan, including $20

[19] https://www.analyticsinsight.net/qnu-labs-launches-quantum-key-distribution-system-and-quantum-random-number-generator-chip/

[20] https://www.wsj.com/articles/colonial-pipeline-hack-sparks-questions-about-lax-cyber-oversight-11620689340?

[21] Executive Order on Improving the Nation's Cybersecurity | The White House

billion for localities to harden energy systems and $2 billion in grants for energy grids in high-risk areas. The recipients of the planned $100 billion broadband investment plan will be asked to source from "trusted vendors."[22]

SolarWinds hackers strike again with phishing attacks

Microsoft Corporation disclosed on May 27 that hackers linked to Russian intelligence SVR, earlier identified for the SolarWinds attacks, seized an email system used by the State Department's international aid agency (USAID) to target human rights groups and other organisations that are critical of President Vladimir V. Putin. The hacker group Nobelium, linked to Russian cyber spy group APT-29, compromised the email marketing service 'the Constant Contact' account and sent out phishing emails with subject lines such as "USAID Special Alert!" that directed victims to a website controlled by hackers. Roughly 3,000 accounts across over 150 organisations in 24 countries, including in the US and Europe, were compromised. The attack was detected only three weeks before President Biden is scheduled to meet President Putin in Geneva. The Kremlin dismissed the Microsoft report, saying that the company's allegations were unfounded.[23]

Ransomware linkages to Crypto currencies

The threat of ransomware has become more serious during the Covid-19 pandemic. The global surge in ransomware attacks has hit a 102 per cent increase in 2021, compared to the beginning of 2020. At least 61 organisations from the Asia Pacific (APAC) region, including Vietnam and India, had been victims of ransomware. Globally, Brazil has been the most affected, followed by Vietnam, South Africa, China, and India.[24]

In the US, the Colonial Pipeline became the latest victim, along with the nearly 2,500 cases reported to the Federal Bureau of Investigation, in which ransomware victims paid hackers $350 million in cryptocurrency. While several solutions to improve cybersecurity have been mooted, an open editorial in the Wall Street Journal of May 25 suggested that a more effective way to stop the global ransomware pandemic would be to ban cryptocurrency. Unless checked, ransomware attacks could target other critical sectors, including power grids or water supply systems. The op-ed suggested a

[22] Joe Biden: Biden administration eyes cybersecurity funding after hacks, IT Security News, ET CISO (indiatimes.com)

[23] https://www.wsj.com/articles/hackers-linked-to-solarwinds-return-with-phishing-attack-microsoft-says-11622222808?st=ccxk4wcj40jtw1p&reflink=article_email_share

[24] https://www.times24h.com/india-china-among-the-most-targeted-regions-for-ransomware-2-0-attacks-in-2020-kaspersky/

collective response with a coherent regulatory framework for cryptocurrency to counteract its use in financing terrorism and facilitating ransomware attacks.[25] Some experts, however, differ with this approach as they opine that the real cybersecurity risks from ransomware are monetary risks; the ban on cryptocurrencies would inhibit innovation. The greater risks associated with taking down or breaking critical infrastructure come from nation-state attacks for geopolitical reasons.[26]

Belgian Government websites suffer DDOS attacks

In Europe, the Belgian government's public-facing websites, internal systems, and other IT networks were shut down by a massive distributed denial of service (DDoS) attack on May 4. The attack disrupted Belnet, a government-funded internet service provider, affecting over 200 entities, including the Belgian parliament, Belgium's official tax filing service and COVID-19 sign-up portal. The situation was brought under control by May 6. In April 2019, the Belgian home ministry was reportedly hacked and government databases were pilfered. Both the attacks reportedly indicated the hands of China.[27]

North Korean Cyber threats are more immediate: US ODNI

Cyber threats from nation states and their proxies have escalated to steal information, influence populations, and damage critical infrastructure. US intelligence agencies remain most concerned about Russia, China, Iran, and North Korea.[28] In the 2021 Annual Threat Assessment Report, released by ODNI on April 13, Washington acknowledged that North Korea "probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks" across the United States. North Korea's nuclear and military programmes are long-term threats, but its cyber threats are immediate, realistic threats.[29]

North Korean hackers have conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide, probably to fund government priorities, such as its nuclear and missile programs. It is assessed that Pyongyang's 6,000-strong cyberwarfare unit, known as Bureau 121, operates

[25] https://www.wsj.com/articles/ban-cryptocurrency-to-fight-ransomware-11621962831

[26] https://www.techdirt.com/articles/20210525/14250246872/babies-bathwater-wsj-oped-suggests-banning-cryptocurrency-entirely-to-stop-ransomware

[27] **https://status.belnet.be/incidents**

[28] https://amp-scmp-com.cdn.ampproject.org/c/s/amp.scmp.com/news/asia/east-asia/article/3134873/north-korean-cyberattacks-more-immediate-threat-its-missiles

[29] The 2021 Annual Threat Assessment Report released by the Office of the Director of National Intelligence

from several countries including Belarus, China, India, Malaysia and Russia, according to a US military report of July 2020.[30]

Social Media vs. Government of Canada

In order to promote domestic content, an amendment to an earlier legislation has been introduced in the Canadian parliament. On May 26, the Canadian Prime Minister stated that the Bill (C-10) aims to level the playing field between Canadian creators and web giants. It requires powerful foreign broadcasters to provide information on their revenues, to contribute financially to Canadian stories and music, and to enable different audiences to experience Canadian culture. It has no impact on Canada's commitment to net neutrality.[31] It mandates video and audio sharing sites to prominently feature more of the country's artists and to contribute more financially to the country's economy. The Canadian government intends to follow Australia in trying to get digital platforms to compensate media outlets for content, and to create a new regulator to police hate speech and other harmful online activity. Canada also plans to levy a digital-services tax starting in 2022.[32]

Artificial Intelligence War

Recent operations by Israel against Hamas have been hailed as the world's first AI war by the Israeli military. The IDF deployed artificial intelligence and supercomputing that were power multipliers in the 11 days of fighting in the Gaza Strip, during which the Israeli military carried out intensive strikes against Hamas and Palestinian Islamic Jihad (PIJ) targets. The IDF established an advanced AI technological platform that centralised all data on terrorist groups in the Gaza Strip onto one system that enabled the analysis and extraction of intelligence. Soldiers in Unit 8200, an Israeli intelligence unit, pioneered algorithms and code that led to several new programs which were developed and used during the fighting. The mapping of Hamas's underground network was done by an all-source intelligence-gathering process, helped by the technological developments and use of Big Data.[33]

[30] https://www.documentcloud.org/documents/7038686-US-Army-report-on-North-Korean-military.html#document/p277/a576734

[31] https://openparliament.ca/bills/43-2/C-10/?tab=mentions&singlepage=1

[32] https://www.wsj.com/articles/canada-wants-youtube-tik-tok-to-prioritize-canadian-content-11622044661?st=z4nkq9ndfo36grg&reflink=article_email_share

[33] https://www.jpost.com/arab-israeli-conflict/gaza-news/guardian-of-the-walls-the-first-ai-war-669371

The US-China technology slugfest

The United States and China are aggressively competing on every aspect of technology and in all geographies. The slugfest has been further sharpened by the coronavirus pandemic, to out-subsidise and out-innovate each other. A recent telecom license auction in Ethiopia took on a wider geopolitical significance over the rollout of 5G. In the auction on May 22, to build a nationwide, 5G-capable wireless network, the Ethiopian government selected a U.S.-backed consortium, led by the U.K.'s Vodafone Group PLC, beating out South Africa's MTN Group Ltd., whose proposal was financed by China.[34]

China is focusing research and investment on "frontier technologies" as it competes for economic superiority with the United States. To maintain its technology edge, subsidies are propelling China's "Made in China 2025" ambitions to lead the future of aerospace, artificial intelligence, automation, biotechnology, digital currencies, electric vehicles, 5G advancements, renewable energy, robotics, semiconductors and creating tech unicorns. In 2020, for example, Xi's government spent a record $33 billion shoring up semiconductors, defence and other sectors pivotal to its tech arms race with the US.[35] It is reckoned that Chinese-made semiconductors will account for 19.4% of the market in 2025. China-based production of general-purpose chips remains a top Xi priority.

The US, on its part, is boosting technology research and increasing chip innovation and production via new subsidies of its own. The Endless Frontier Act, substituted by the United States Innovation and Competition Act (USICA) of 2021, which aims to counter the rise of China's technological power, was tabled before the U.S. Senate on May 17. The USICA establishes a Directorate of Technology and Innovation at the National Science Foundation. It authorises $81 billion for the NSF, including $29 billion over five years for the new directorate. It directs the Department of Commerce to designate regional technology hubs across the country, and authorises $10 billion over five years for these hubs. The bill appropriates $52.7 billion for incentivising domestic semiconductor fabrication and $1.5 billion for 5G innovation.[36]

The real drive of the United States is to win the technology race with China, thereby avoiding a new international tech order under Beijing's control, without losing the massive market of China.

[34] https://www.wsj.com/articles/u-s-china-tech-fight-opens-new-front-in-ethiopia-11621695273

[35] https://menafn.com/1102108662/US-China-in-the-right-kind-of-tech-war

[36] https://www.rpc.senate.gov/legislative-notices/s1260_the-united-states-innovation-and-competition-act

International Cooperation

India-EU Leaders' Meeting

The leaders of the European Union (EU) and its Member States met in hybrid format on May 8, in the EU's first ever meeting with India in the EU+27 format. Summit leaders agreed to strengthen the "India-EU Strategic Partnership". On the digital front, both sides called for early operationalisation of the Joint Task Force on Artificial Intelligence, closer cooperation on global digital standards, and network security, including in relation to 5G technology and beyond 5G. Both sides also agreed to deepen technological cooperation on Quantum and High-Performance Computing and looked forward to an outcome oriented High-Level India-EU Digital Investment Forum meeting in 2021.[37]

India-UK Virtual Summit

At the India-UK virtual summit held on May 4, a Joint Declaration of Intent on cooperation in the Digital and Technology fields was concluded to deepen cooperation on emerging technologies, digital infrastructure, and data policies. A MOU on cooperation in the field of telecommunication/ICT between India and the UK was also signed.[38]

[37] https://mea.gov.in/bilateral-documents.htm?dtl/33853/Joint_Statement_on_IndiaEU_Leaders_Meeting_May_08_2021

[38] https://mea.gov.in/bilateral-documents.htm?dtl/33840/List_of_MoUsDeclarations_agreedannounced_at_the_IndiaUK_Virtual_Summit_May_4_2021

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

www.delhipolicygroup.org