Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

SEPTEMBER 2021

Volume II, Issue 9 | September 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 9
September 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 9
September 2021

Contents

Abstract i
National Developments 1
China continues to pose cyber security threats to India 1
Government announces major telecom reforms package 1
Telecom reforms and PLI to boost innovations for 5G 2
Concerted efforts by India to build semiconductor industry 2
Army orders tactical drones on fast track 3
Parliamentary panel meets on the Personal Data Protection Bill 4
Supreme Court to pronounce order on Pegasus Row shortly 4
India's KOO app clocks 10 million downloads 5
Capability Building for Innovative Cyber Security Products 5
International Developments 6
U.S. Sanctions Crypto Exchange aiding Ransomware Criminals 6
Turmoil in Russian Cyber Space 6
Saudi Arabia approves new Personal Data Protection law 6
Pakistan plans to roll out 5G in 2023 7
China Declares Cryptocurrency Transactions Illegal 7
Global efforts to meet Semiconductor Chip shortage 8
International Cooperation 10
Centrality of emerging technologies in Quad Summit 10
SCO Council of Heads of State meet in Dushanbe 11
Bilateral meets on Cyber Security and technologies 11

Abstract

September did not witness high-profile cyberattacks, but threats from China continued, targeting Indian media networks and government organisations. The Indian government unveiled a far-reaching Telecom Reforms Package designed to spur growth, innovation and investment. This package, along with the production-linked incentive (PLI) scheme and innovations for 5G networks, carries the potential to reduce the share of telecom imports to under 50%. India is also making concerted efforts to invite investments in the Chip manufacturing sector, which is at the core of cyber security. Amidst the standoff with China on the LAC, the Indian Army is fast-tracking manufacture of tactical drones in collaboration with Indian start-ups and foreign entities.

On the international front, the US imposed sanctions on a Russia based crypto currency exchange, to deter ransomware gangs from laundering money through crypto currencies. Post the Biden-Putin summit, the Russian internet space has seen a lot of turmoil, including internet outages and the arrest of the CEO of a cyber security firm.

Privacy and data protection have become global concerns. While India is still deliberating on the Personal Data Protection Bill, Saudi Arabia has enacted a personal Data Protection Law. Talks are on between the US and the EU to ease trans-Atlantic data flows, after a European court invalidated the 'Privacy Shield' in 2020. Amidst regulatory tightening of the technology and real estate sectors, China has made cryptocurrency-related transactions illegal, citing the need for national security and stability.

During the month, India participated in important summits of the Quad, SCO and BRICS, in each of which there was focus on development of emerging technologies, supply chain resilience, cyber-crimes and cyber security.

National Developments

China continues to pose cyber security threats to India

Since the border standoff between India and China began in May 2020, Chinese hacker groups have been regularly targeting Indian public sector companies and technical establishments through cyber security breaches. As of early August 2021, there has been a 261% increase in the number of suspected state-sponsored Chinese cyber operations.[1] The US based Insikt Group published a report on September 22, indicating that Chinese hackers had launched a series of cyber-attacks against high profile Indian targets including Bennett Coleman & Co. Ltd., parent of the Times media Group, the UIDAI (Unique Identification Authority of India) and the Madhya Pradesh Police department. Reportedly, 500 megabytes of data was extracted from the Times network. The hacking group, named TAG-28, made use of 'Winnti' malware, which is shared among several Chinese state-sponsored activity groups.

On September 23 TALOS, CISCO's Cyber Security Research team, revealed that Indian government and defence officials were under Cyber-attack since late 2020. These attacks were primarily on the users of 'kawach', a two-factor authentication tool used by the National Informatics Centre (NIC).[2]

Unlike the standard approach of spywares and Advanced Persistent Threats (ATPs), the motivated actors used off-the-shelf Remote Access Trojans (RATs) by phishing attack, in which the victims are lured to open malicious documents of interest.

Government announces major telecom reforms package

The telecom sector is the backbone for Digital India. However, lack of innovation due to financial constrains had plagued the sector. Therefore, the announcement of the liberalised Telecom Reforms Package by the Indian government on September 15 is considered timely for its growth and security. The Package includes nine structural reforms and five procedural reforms, along with several financial relief measures for the Telecom Service Providers (TSP).

Among these major structural reforms are the rationalisation of Adjusted Gross Revenue (AGR) by excluding non-telecom revenue; huge reduction in Bank Guarantee (BG) requirements (80%) against License Fee (LF); increase in tenure

[1] https://indianexpress.com/article/world/china-hack-bennett-coleman-times-of-india-madhya-pradesh-7528820/
[2] https://www.digital-secure.in/post/opeartion-armor-piercer

of spectrum from 20 to 30 years in future auctions; no Spectrum Usage Charge (SUC) for spectrum acquired in future spectrum auctions; and above all,100% Foreign Direct Investment (FDI) under the automatic route in the Telecom Sector with all safeguards.

Procedural Reforms include fixation of a spectrum auction calendar; liberalisation of 'Know Your Customers' (KYC) and e-KYC rules; easing of clearance for telecom towers by the Standing Advisory Committee on Frequency Allocation (SACFA); and promotion of ease of doing business.

The Indian Cabinet also approved measures to address liquidity requirements of all Telecom Service Providers (TSPs) that include moratorium/deferment of up to four years in annual payments of dues arising out of the Adjusted Gross Revenue (AGR) judgement; moratorium/deferment on due payments of spectrum purchased in past auctions (excluding the auction of 2021) for up to four years; and option to the TSPs to pay the interest amount arising due to the said deferment of payment by way of equity, guidelines which will be finalised by the Ministry of Finance.[3]

Telecom reforms and PLI to boost innovations for 5G

The Telecom Reforms package along with the production-linked incentive (PLI) scheme and open radio access network (O-RAN) for 5G has the potential to reduce the share of telecom imports to under 50%. On September 6, it was reported that the government has approved 33 companies for the PLI scheme for the telecom sector and networking equipment, to boost local production of telecom equipment, reduce dependency on imports and make India a global manufacturing hub by incentivising companies making in India. The Telecom Reforms Package with provisions of 100% FDI is expected to attract further investments for manufacturing of network equipment, routers, broadband transmission equipment, 5G equipment and other electronics items. The advent of O-RAN, by disaggregating hardware and software at radio sites, would allow domestic equipment makers to manufacture and innovate.[4]

Concerted efforts by India to build semiconductor industry

The global shortage of chips that has disrupted production of smart phones and cars is also affecting India. Reliance Jio has delayed the launch of its smartphone while major automakers, including Maruti Suzuki, Tata and Mahindra and Mahindra, have stalled production. Expansion of Indian 4G

[3] Press Information Bureau (pib.gov.in)
[4] https://www.businesstoday.in/industry/telecom/story/pli-scheme-for-telecom-sector-govt-to-approve-proposals-of-33-companies-306006-2021-09-06

networks may be delayed by six months, resulting in network congestion, if the global shortage of semiconductors and component supply chain challenges persist. Concerted efforts are being made to boost semiconductor Chip supply.

On September 23, PM Narendra Modi discussed this issue with the chief executives of US technology companies and invited them to 'Make in India' by highlighting opportunities offered by India's telecom and electronics sector, including the PLI scheme for Electronics System Design and Manufacturing (ESDM) for the manufacture of Chips.

Meanwhile, a joint Semiconductor Supply Chain Initiative (SSCI) has been launched by the Quad partners. India is also looking towards Taiwan, with whom it has been hesitant to deal earlier for geo-political reasons. It was reported on September 27 that India and Taiwan are in talks on a deal that would bring a Chip plant worth an estimated $7.5 billion to India to supply everything from 5G devices to electric cars. India is currently studying possible locations with adequate land, water and manpower, while indicating possible financial support of 50% of capital expenditure with tariff reductions on components for producing semiconductors and other incentives. The agreement would be a win-win situation for both, as India seeks technology investments to become self-reliant on chips, while Taiwan wants to strengthen its diplomatic presence around the globe to ward off pressures from China.[5]

Earlier, on September 5, it was reported that the government received applications from 20 top companies after it floated the Expression of Interest (EoI) to set up semiconductor plants in the country. These include a bid by Tata Sons and a consortium floated by Abu Dhabi-based Next Orbit Ventures, that includes Israel based Tower Semiconductor, which has pitched for a $3 billion analogue 65 nanometre semiconductor fabrication unit (Fab) in Gujarat. It is learnt that the Indian government is prepared to subsidise as much as 40-50% of the cost of setting up Fabs, for both traditional and advanced Chips. The government will soon put out a request for proposal (RFP) document seeking formal applications from companies.[6]

Army orders tactical drones on fast track

On September 3, it was reported that the Army has ordered over 100 tactical "kamikaze" Israeli drones, amidst the continuing standoff with China and Pakistan along the LAC and LOC. The loitering munition 'SkyStriker' will be

[5] https://www.livemint.com/news/india/india-accelerates-talks-with-taiwan-on-chip-plant-trade-deal-11632704065463.html

[6] https://telecom.economictimes.indiatimes.com/news/leading-global-chip-foundry-tower-semiconductor-wants-govt-to-finalise-project-sops/86055853

manufactured in Bengaluru by a joint venture between Israel's Elbit System and India's Alpha Design. It carries a warhead of 5-10 kgs and is capable of hitting moving targets and armoured personnel carriers.[7]

In another procurement, the Indian Army has awarded a Bengaluru-based startup, Newspace Research & Technologies, a $15 million contract to supply 100 swarm drone units. NewSpace Research is working with Hindustan Aeronautics Ltd. for a futuristic air-launched swarm drone system, called Combat Air Teaming System (CATS), which envisages a manned aircraft capable of launching multiple drones to carry out high-risk missions, including taking down of enemy air defences.[8]

Given its traditional strengths in innovation, information technology, frugal engineering and its huge domestic demand, India has the potential of becoming a global drone hub by 2030. The PLI scheme, along with the recently announced liberalised Drone Rules, 2021 should trigger investments in this sector.[9]

Parliamentary panel meets on the Personal Data Protection Bill

On September 29, The Joint Parliamentary Committee deliberated on the clauses of the much-awaited Personal Data Protection Bill and sought clarity and amendment of a contentious clause which in the name of "sovereignty", "friendly relations with foreign states" and "security of the state", gives powers to the Central government to suspend all or any of the provisions of the Act to make exemptions for government agencies. The committee advised that the conditions for making the exemptions should be clearly laid down without leaving scope for interpretation, and the clause needs to be appropriately amended. The Bill is expected to be tabled during the Winter session of the Parliament.[10]

Supreme Court to pronounce order on Pegasus Row shortly

The Supreme Court, on September 23, pronounced its intention to set up a committee of technical experts to look into allegations of unauthorised surveillance using the Pegasus software made by Israeli firm NSO Group. The

[7] Army orders over 100 Indo-Israeli kamikaze drones amid active LAC and precarious LoC (ampproject.org)
[8] swarm drones: India places orders for drones, loitering munitions - The Economic Times (indiatimes.com)
[9] Auto sector, drone PLIs: Green light for new-age tech - The Economic Times (indiatimes.com)
[10] Data Protection Law | Clearly define exemptions to government agencies, says parliamentary panel - The Hindu

final order, naming the expert team, will be made shortly. Earlier on September 13, the Indian government had expressed reservations on making a public affidavit as this issue is fraught with questions of national security.[11]

India's KOO app clocks 10 million downloads

It was reported on August 26 that the indigenous, multi-language and microblogging app, Koo, has crossed 10 million downloads since its launch in March 2020. The app gained prominence during the face-off between Twitter and the Indian establishment. Koo is currently available in eight languages — Hindi, Kannada, Marathi, Tamil, Telugu, Assamese, Bangla and English. The app is also available in Nigeria, which banned Twitter in June.[12]

Capability Building for Innovative Cyber Security Products

The Interdisciplinary Centre for Cyber Security and Cyber Defence of Critical Infrastructures (C3I) at IIT Kanpur has built India's first cyber security test bed to discover cyber threats to critical infrastructure, develop solutions, and alert the National Cyber Security Coordinator (NCSC) and other government agencies. The Centre has invited applications by September 15 from all innovators in Cyber Security in the domains of UAV security, blockchain, intrusion detection, and cyber physical system, for its 2nd Start-up Cohort Program. The first cohort included 13 start-ups and 25 R&D Principal Investigators for the Incubation and Research programme.[13]

[11] https://indianexpress.com/article/india/pegasus-row-sc-to-pronounce-order-next-week-7529112/

[12] Koo app clocks 1 crore downloads in less than 18 months of operations - The Economic Times (indiatimes.com)

[13] Fuel Your Dreams: C3ihub At IIT Kanpur Invites Entrepreneurs To Build Innovative Cyber Security Products - The420CyberNews

International Developments

U.S. Sanctions Crypto Exchange aiding Ransomware Criminals

In order to deter criminal ransomware attacks on businesses and critical infrastructure, on September 21 the US administration imposed sanctions against a Russia-based cryptocurrency exchange, SUEX-OTC, accused of handling ransomware payments in virtual currency. SUEX had processed payments of more than $481 million in bitcoin, mostly linked to people operating on the dark web and ransomware gangs.[14] The Treasury Department sanctions prohibit U.S.-based firms from doing business with the firm and blocks any assets it has within US jurisdiction. It also sets the stage for a broader sanctioning of the crypto sector, in collaboration with international partners, to weed out money laundering of ransomware payments by criminals.

Turmoil in Russian Cyber Space

On September 8, it was reported that the Russian internet giant Yandex had been hit by a distributed denial-of-service (DDoS) attack, in which hackers attempt to flood a network with unusually high volumes of data traffic in order to paralyse it. The cyber-attack was repelled by the company and presumably did not impact its services and user data.[15] Coincidentally, on September 8, several websites linked to jailed opposition politician Alexei Navalny were affected, causing major outages of the internet, presumably due to the Kremlin's crackdown to prevent access to a banned app backed by Navalny's allies.[16]

On September 29, Russia detained the head of one of the country's largest cyber-security firms, the IB Group, on treason charges for working with the West to combat cyber-attacks. The IB Group, founded in 2003, specialises in the identification and prevention of cyber-attacks and collaborates with Interpol and other global agencies. The company denied cooperation with "intelligence agencies of foreign powers."[17]

Saudi Arabia approves new Personal Data Protection law

While India is still deliberating on the Personal Data Protection Bill, on September 14, Saudi Arabia enacted a Personal Data Protection Law. The law,

[14] https://www.wsj.com/articles/u-s-treasury-threatens-more-sanctions-targeting-crypto-services-found-aiding-illicit-actors-11632234624?mod=itp_wsj&mod=djemITP_h
[15] Russian Tech Giant Yandex Says It Was Targeted In Biggest Attack Ever (rferl.org)
[16] https://chanakyaforum.com/kremlin-internet-crackdown-causing/
[17] Possible Global Pressure? Russia Detains Country's Top Cybersecurity CEO For Treason - The420CyberNews

which protects personal data from unconsented collection and processing, is to be implemented within six months. The Saudi Data and Artificial Intelligence Authority (SDAIA) has been designated to protect any personal data that might lead to identifying, directly or indirectly, the user from unconsented collection and processing. The protected data includes name, identification number, address, phone number, personal records, financial records and images, videos or any other identifying data. The law will ensure the privacy of personal data, regulate the sharing of personal data and prevent the abuse of personal data.[18]

Data privacy has become a major contentious issue across the world. On September 29, the US-EU Trade and Technology Council met in Pittsburgh to strike a deal to ease trans-Atlantic data flows. The high-level meeting was intended to ease recent tensions and help coordinate their approaches to issues such as export controls, technology regulation and data governance. The new agreement is crucial to transfer data out of the European Union to the US, after a European court invalidated a previous agreement known as the 'Privacy Shield' in 2020.[19]

Pakistan plans to roll out 5G in 2023

On September 7, the Dawn newspaper reported that Pakistan is aiming to roll out 5G in 2023. For future digitisation and new technologies such as 5G, "deep fiberisation" projects have been launched by the Universal Service Fund (USF), on which the Pakistan government is banking heavily on increasing exports of IT services up to USD 5 billion by the end of 2022-23. According to its IT & Telecom ministry, the spectrum auction for Pakistan-occupied Kashmir (POK) and Gilgit-Baltistan for next generation mobile services will help improve the telecom and broadband services while the USF projects would cover over 1,800 km of unserved road network, including highways and motorways, in Baluchistan.[20]

China Declares Cryptocurrency Transactions Illegal

On September 24, the People's Bank of China announced that all cryptocurrency-related transactions are illegal, to further prevent the risks surrounding crypto trading and to maintain national security and social stability. The central bank said on its website that cryptocurrencies are issued by non-monetary authorities, use encryption technologies and exist in digital

[18] cybersecurity: Saudi Arabia approves new law to protect personal data, IT News, ET CIO (indiatimes.com)
[19] https://www.wsj.com/articles/data-privacy-impasse-hangs-over-u-s-eu-trade-and-technology-summit-11632948689
[20] https://www.thehindubusinessline.com/news/world/pakistan-plans-to-roll-out-5g-in-2023/article36331547.ece

form and shouldn't be circulated and used in the market as currencies. This reinforces the country's push to develop a state-backed digital currency while taking a tough stance against crypto currencies that it believes facilitate money laundering and illegal capital outflow.[21]

China banned cryptocurrency exchanges from operating within its borders several years ago, but it tolerated crypto mining, which uses high-powered computers to generate the digital currencies that people invest in and trade. These operations were often powered by cheap electricity in coal-rich regions of Xinjiang and Inner Mongolia, along with the hydropower centres of Sichuan and Yunnan. The crackdown has prompted an exodus of crypto miners to other countries, including the US and Kazakhstan.

Global efforts to meet Semiconductor Chip shortage

While the US is struggling to cope with semiconductor chip shortages, several technology giants in the US, EU and Asia are trying to set up new plants with subsidies and incentives from respective governments. The shortage is also giving rise to investment in companies whose products include small parts called substrates, which connect chips to the circuit boards that hold them in personal computers and other devices.[22] On September 6, Qualcomm announced that it will supply a key computing chip for the digital dashboard in a new Renault SA electric vehicle. Samsung Electronics is planning for a $17 billion chip plant in the city of Taylor, Texas. This site is in addition to Austin, where Samsung owns its sole US chip factory. Intel plans to invest up to $95 billion in European chip-making amidst its US Expansion. On September 7, Intel reported that it was planning two chip factories at a new site in Europe. Intel rival TSMC has purchased land to build its first US campus in Phoenix, where TSMC plans up to six chip factories [23] Huawei is trying to circumvent the US ban on 5G technology by ordering from Qualcomm the 4G Snapdragon Chips, without support for 5G.[24]

To complement private sector efforts, the European Commission announced plans on September 15 for a new European Chips Act to keep the EU competitive and self-sufficient. The European Chips Act would encompass research, production capacity and international cooperation, and envisages

[21] https://www.wsj.com/articles/china-declares-bitcoin-and-other-cryptocurrency-transactions-illegal-11632479288?mod=djemalertNEWS
[22] https://www.wsj.com/articles/a-big-hurdle-to-fixing-the-chip-shortage-substrates-11630771200?action=profile_completion&
[23] https://telecom.economictimes.indiatimes.com/news/intel-breaks-ground-on-20-bln-arizona-plants-as-u-s-chip-factory-race-heats-up/86499533
[24] Huawei escapes U.S. chip ban by buying 4G Snapdragon chips instead of 5G - PhoneArena

that the EU should look into setting up a dedicated European Semiconductor Fund. European leaders have also pushed for financial inducements as part of a goal of doubling Europe's share of global chip-making capacity to 20% over the next decade.[25] The United States had last year announced its CHIPS for America Act aimed at boosting its ability to compete with Chinese technology.

[25] 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

Centrality of emerging technologies in Quad Summit

On September 24, the Leaders of the Quad countries (Australia, India, Japan, and the United States of America) met in person to establish cooperation on critical and emerging technologies, and committed to work together to facilitate public-private cooperation and demonstrate in 2022 the scalability and cybersecurity of open, standards-based technology. Quad leaders also recognised the centrality of emerging technologies in shaping the 21st-century global order.[26] They launched the Quad Principles on Technology Design, Development, Governance, and Use that will guide not only the region but the world toward responsible, open, high-standards innovation. The Quad principles envisage building trust, integrity, and resilience; and foster healthy competition and international collaboration to advance the frontier of science and technology.[27]

The Quad further launched Technical Standards Contact Groups on Advanced Communications and Artificial Intelligence focusing on standards-development activities as well as foundational pre-standardisation research. A joint Semiconductor Supply Chain Initiative (SSCI) was also launched to map capacity, vulnerabilities and bolster supply-chain security for semiconductors and their vital components.

On 5G, Quad leaders supported fostering and promoting a diverse, resilient, and secure telecommunications ecosystem. They launched a Track 1.5 industry dialogue on Open Radio Access Network (O-RAN) deployment and adoption, to facilitate enabling environments for 5G diversification, that has a strong geopolitical imperative - keeping closed networks at bay and opening up a vendor agnostic ecosystem.[28]

To collaborate on cyberspace, the Quad will launch new efforts to bolster critical-infrastructure resilience against cyber threats by creating a Quad Senior Cyber Experts Group that will meet regularly to advance work between government and industry to adopt and implement shared cyber standards; development of secure software; building workforce and talent; and promoting

[26] https://www.mea.gov.in/bilateral-documents.htm?dtl/34323/Quad_Principles_on_Technology_Design_Development_Governance_and_Use
[27] https://www.mea.gov.in/bilateral-documents.htm?dtl/34318/Joint_Statement_from_Quad_Leaders
[28] https://www.mea.gov.in/bilateral-documents.htm?dtl/34319/Fact_Sheet_Quad_Leaders_Summit

the scalability and cybersecurity of secure and trustworthy digital infrastructure.[29]

SCO Council of Heads of State meet in Dushanbe

On the twentieth anniversary of the founding of the Shanghai Cooperation Organisation (SCO), member states including India, China and Russia met in a hybrid mode in Dushanbe on September 17. While the major discussions were on Afghanistan, regional security, combating terrorism, extremism, separatism and fight against organised crime, member States noted with serious concern the growing threats to information security, including the criminal misuse of information and communication technologies, which are destabilising international peace and security. They decided to build practical cooperation in the field of international information security based on the relevant Cooperation Plan for 2022-2023 and other documents adopted by the Organisation.

The SCO summit also committed members to cooperate in the relevant negotiation mechanisms at the UN and other international fora for the development of universal rules, principles and norms of responsible behaviour of states in cyberspace, including the launch of a comprehensive international convention on combating the use of ICTs for criminal purposes. They advocated equal rights for all countries to regulate the Internet and the sovereign right of states to manage it in their national segment.[30]

Bilateral meets on Cyber Security and technologies

On the sidelines of the Quad in-person summit, the Indian PM had important bilateral meetings on September 23 with the PMs of Australia and Japan, and on September 24 with the US President. In the statement issued after the India-US bilateral summit, both countries decided to expand their partnership in new domains and several areas of critical and emerging technologies, including space, cyber, health security, semiconductors, Blockchain, AI, 5G, 6G and future generation telecommunications technology. They recognised the foundational need to address vulnerabilities and threats in cyberspace, including to promote critical infrastructure resilience, and welcomed the

[29] https://www.mea.gov.in/bilateral-documents.htm?dtl/34319/Fact_Sheet_Quad_Leaders_Summit
[30] Dushanbe Declaration on the Twentieth Anniversary of the Shanghai Cooperation Organisation (mea.gov.in)

increasing partnerships among governments to counter ransomware and other cyber-enabled trans-border crimes.[31]

In their bilateral meeting on September 23, the Prime Ministers of India and Japan discussed the COVID-19 pandemic and efforts to address it; evaluated the progress in the India-Japan Digital Partnership, especially in start-ups; exchanged views on further collaboration in various emerging technologies; and welcomed the launch of the Supply Chain Resilience Initiative (SCRI) between India, Japan and Australia earlier this year as a collaborative mechanism to enable resilient, diversified and trustworthy supply chains.[32]

In the bilateral between the Indian and Australian PMs on September 23, the leaders noted with satisfaction the regular high-level engagements between the two countries, including the recently held first India-Australia Foreign and Defence Ministers' 2+2 Dialogue.[33]

On September 23, PM Modi also met leading CEOs from five technology sectors that include drones, 5G, semiconductors and solar.[34] He invited them to develop standards and technology and make technology investments taking advantage of incentives and recent reforms announced by India.[35] While the meeting with Adobe reflected the priority for Digital India, the meeting with General Atomics was significant as the company is the pioneer in military drone technologies and is the world's top manufacturer of state-of-the-art military drones. The meeting with chip giant QUALCOMM signified India's push for 5G technology that is safe and secure.[36]

[31] U.S.-India Joint Leaders' Statement: A Partnership for Global Good (September 24, 2021) (mea.gov.in)
[32] Meeting between Prime Minister Shri Narendra Modi and H.E. Mr. SUGA Yoshihide, Prime Minister of Japan (mea.gov.in)
[33] Prime Minister's meeting with Australian Prime Minister Scott Morrison on the sidelines of the Quad Leaders' Summit (mea.gov.in)
[34] PM Modi meets Kamala Harris, Suga, Morrison on Day 2 in US; top-3 developments (livemint.com)
[35] https://www.livemint.com/news/india/modi-in-us-pm-meets-leading-american-ceos-from-key-sectors-11632406187077.html
[36] https://www.indiatvnews.com/news/world/prime-minister-narendra-modi-meeting-ceos-qualcomm-adobe-first-solar-general-atomics-blackstone-united-states-pm-modi-us-visit-2021-735904

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

www.delhipolicygroup.org