Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

APRIL 2021

Volume II, Issue 4 | April 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 4
April 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 4
April 2021

Contents

Abstract

Data has become the most precious commodity for technology companies, nation states and criminal elements. During the month, data from six Indian enterprises was put on sale on the dark web. Mining of personal data is being resorted to by state sponsored hackers to trigger attacks on adversaries, while digital companies are tweaking their privacy rules to capitalise on data for advertisements and profit.

India plans to enhance its broadband penetration by adopting satellite broadband internet services from several global satellite operators. Actions are in hand to facilitate secure and faster satellite connectivity.

The US formally attributed the SolarWinds cyber-espionage campaign to the Russian Foreign Intelligence Service (SVR) and announced a number of retaliatory measures against Russia, including economic sanctions against individuals, entities and the expulsion of diplomats.

In his Address to a joint session of Congress on April 28, President Biden called for huge federal investments of $2.3 trillion in infrastructure development, including $100 billion for broadband connectivity, $50 billion for semiconductor research and manufacturing, and another $50 billion for the National Science Foundation for technology development.

A planned cyber-attack on Iran's Natanz uranium enrichment site caused a power failure, but failed to derail diplomatic efforts to salvage the 2015 nuclear deal, with discussions being held in Vienna, on April 17.

The EU has proposed a regulatory framework for the use of artificial intelligence, to address human and societal risks, while strengthening AI uptake, investment and innovation across Europe.

The US and Japan have entered into a Competitiveness and Resilience (CoRe) Partnership focussed on digital technologies, among other contemporary issues. These include development, testing, and deployment of secure 5G and next-generation mobile networks ("6G" or "Beyond 5G"), with a combined commitment of $ 4.5 Billion.

National Developments

The Cyber Threat Scenario

In the first four months of 2021, there have been large-scale data leaks of personally identifiable information on the Dark Web. As many as six data breach cases that occurred over the last three months were reported on April 18. These include credit card details of nearly 10 lakh customers of Domino's Pizza India, worth 13 TB, allegedly being sold for $550,000 on the Dark Web. Other data thefts include 8.2 TB of data of Mobikwik users, data on 30 million users of LinkedIn India and data on 6 million users of Facebook-India. Indian mobile data has also become vulnerable. India has seen a 845% jump in cyberattacks on mobile devices between October 2020 and March 2021.These mobile devices are inherently vulnerable to cyber-attacks due to flaws in their chipsets, and need urgent patching.[1]

To mitigate threats, on April 19, CERT-In has advised Facebook users to strengthen their account privacy settings after the recent global 'data scraping' incident in the social media platform.[2] RBI has advised Mobikwik to carry out a third-party forensic audit by empaneled auditors.

Social Media and National Security

Amidst several scathing columns written internationally and negative narratives in social media about the government's response to the second wave of the Covid-19 crisis, the Indian government ordered Twitter Inc., Facebook Inc. and Instagram to block about 100 social media posts, criticising their handling of the pandemic in the country. The legally binding order, under the IT Act, was designed to tackle attempts in recent days to spread coronavirus-related misinformation and create panic by posting images of dead bodies taken out of context. Twitter, which received many of the takedown requests, blocked the posts in India, though they remained visible outside the country.[3] Facebook Inc. had temporarily blocked certain posts, on their own accord, which were later restored. On April 30, the Indian Supreme Court warned State governments and police against clamping down on the spread of information

[1] https://telecom.economictimes.indiatimes.com/news/india-sees-845-jump-in-cyber-attacks-on-mobile-devices-between-oct-2020-and-mar-2021-check-point/82062135
[2] CERT-In Advisory CIAD-2021-0017
[3] https://www.wsj.com/articles/india-accused-of-censorship-for-blocking-social-media-criticism-amid-covid-surge-11619435006

or calls for help through social media from citizens affected by the unprecedented second wave of COVID-19.[4]

The petition by social media platforms, Facebook and WhatsApp, challenging an order of India's competition regulator, the Competition Commission of India (CCI), directing a probe into WhatsApp's new privacy policy, was dismissed by the Delhi High Court on April 22. The court saw no merit in the petitions to interdict the investigation directed by the CCI on March 24, for breaching the Competition Act, 2002.[5]

Satellite Broadband Plans

As of June 2020, India has a Broadband Internet subscriber base of 698.23 million and Narrowband Internet subscriber base of 50.84 million.[6] These figures can be substantially increased by Satellite-based broadband internet, which can also become the backbone for networks of Internet of Things (IoT) devices, smart factories, utilities and other systems in remote areas. While the Government is working on smart delivery and consumption of such services, global satellite providers are competing to access the Indian market.

On April 25, OneWeb launched a set of 36 satellites, taking its total count in lower earth orbit (LEO) to 182 satellites. These would form part of OneWeb's 648 LEO satellite fleet that will deliver high-speed, low-latency global connectivity. OneWeb intends to make global service available next year, including in India. Similarly, SpaceX has started offering the beta version of its Starlink satellite internet service on pre-orders in India for a fully refundable deposit of $99.

To enhance broadband connectivity to rural and remote areas, India needs to facilitate a level playing field for telecom and satellite operators. Regulatory bottlenecks need to be addressed for faster and cheaper satellite connectivity services, with leased bandwidth capacity directly from foreign satellite operators. Towards this end, on April 9, the Department of Telecommunications issued an amendment to VSAT licenses[7], while last month it had amended the provision and operation of satellite-based services using Network equipment from 'trusted sources' and through gateways installed in India.[8] Foreign operators offering the satellite internet service in India need to comply with the laws of the land and licensing conditions need

[4] https://www.thehindu.com/news/national/dont-clampdown-dissemination-of-information-on-covid-19-supreme-court-tells-centre-states/article34447671
[5] https://telecom.economictimes.indiatimes.com/news/delhi-hc-dismisses-facebook-whatsapp-pleas-against-cci-order-to-probe-privacy-policy/82192846
[6] https://trai.gov.in/sites/default/files/Report_09112020_0.pdf
[7] captive vsat.pdf (dot.gov.in)
[8] https://www.voicendata.com/dot-extends-telecom-equipment-procurement-changes-to-satellite-services/'

to be set out in coordination between the Department of Telecommunication and the Department of Space. These would need further policy clarity to allay any concerns around national security.[9]

India working on 5G standards with EU

India plans to work with the EU for building common standards to ensure security across the 5G value chain, as concerns grow about the dominance of Chinese telecom giants. The European Union will discuss 5G technology rollouts and the establishment of global security standards when its leaders meet with Indian counterparts on May 8, for discussions on trade and security issues. Standards would include agreeing on technical aspects like radio spectrum bands, interface technologies to be used by 5G networks and creating level-playing fields for local and smaller companies.[10]

5G signal station near the Tibet border

The Chinese military's official website reported on April 12 that it has opened a 5G signal base at the world's highest Ganbala radar station in the remote Himalayan region of Tibet, which is the world's highest manually operated radar station at an elevation of 5,374 meters. The mountain is located in Nagarze County in Tibet, which is in the vicinity of borders with India and Bhutan. At the end of last year, the People's Liberation Army started to coordinate with civilian enterprises to launch the 5G base station construction in Ganbala to solve the difficulty of network access for the border defence troops, the website said.[11]

Employment of Artificial Intelligence by Armed Forces

The Indian Armed Forces have plans to embrace the next generation (5G) technology to bring Artificial Intelligence-assisted next-gen technologies and unmanned vehicles to centre stage. The Defence Ministry has established a high-level Defence AI Council (DAIC) tasked to provide strategic direction towards the adoption of AI in defence. The DAIC will guide the partnership between the government and industry under the Defence AI Project Agency (DAIPA) as its central executive body. It would also review ethical, safe and

[9] https://telecom.economictimes.indiatimes.com/news/global-local-players-seek-ways-to-lower-cost-of-satellite-broadband-services/82257079
[10] https://telecom.economictimes.indiatimes.com/news/eu-official-looks-to-align-with-india-on-5g-to-protect-democracy/82145464
[11] https://telecom.economictimes.indiatimes.com/news/china-opens-5g-signal-station-at-worlds-highest-radar-location-near-tibet-border/82034096

privacy assured usage of AI in defence.[12] On April 5, the Chief of the Indian Air Force (CAS) indicated that Artificial intelligence would be employed for threat monitoring in the Indian Air Force's captive networks, including the current network upgrades. The Air Force is working on AI based predictive maintenance and predictive threat scenarios. The Air Force has improved operation efficacy by shrinking timelines in the entire chain.[13]

Incentives for Semiconductor chip manufacturing companies

With the success of the 'Make in India' drive that has helped to turn India into the world's second-biggest mobile manufacturer after China, India now seeks to strengthen its electronics supply chain by incentivising chip manufacturing units in India. In December 2020, India had invited an "expression of interest", to be submitted by March 31, 2021 from chipmakers for setting up fabrication units in the country or for the acquisition of such manufacturing units overseas by an Indian company or consortium. The Indian government announced its offer to provide cash incentives of more than $1 billion to each such company. It is estimated that it would cost roughly $5-$7 billion to set up a chip fabrication unit in India and take 2-3 years after all approvals.

A consortium of investors led by Abu Dhabi-based fund Next Orbit Ventures has shown interest in setting up in India. Moreover, Indian conglomerates, such as the Tata Group, have also expressed interest.[14] Chips made locally will be designated as "trusted sources" and can be used in products ranging from CCTV cameras to 5G equipment.

[12] https://www.newindianexpress.com/nation/2019/sep/25/army-to-use-artificial-intelligence-within-2-3-years-to-get-more-lethal-edge-2039052.html
[13] https://ciso.economictimes.indiatimes.com/news/iaf-to-use-ai-aided-tech-for-threat-monitoring-in-captive-networks-chief/81932521
[14] https://telecom.economictimes.indiatimes.com/news/a-billion-for-every-chip-maker-who-makes-in-india-sources-say/81776742

International Developments

Activities in Global Cyber Space

In response to recent challenges from adversaries in the US cyberspace, on April 15 President Biden announced retaliatory measures against Russia over election interference, the SolarWinds cyberattack and other malign activity. The Executive Order (EO) formally attributed the SolarWinds cyber espionage campaign to the Russian Foreign Intelligence Service (SVR), based on an analysis by the Cyber National Mission Force (CNMF). Retaliatory actions included expulsion of ten Russian diplomats and imposing sanctions against dozens of companies and individuals. The most significant economic sanction was to stop American financial firms from dealing in newly issued Russian debt, after June 14, to complicate Moscow's ability to raise money in international capital markets.[15] It is interesting to note that ten of the 32 individuals and entities sanctioned by the US are based in Pakistan.

The EO also included steps to strengthen US and allies' cyber defense. As a follow up, the U.S. Senate Select Committee on Intelligence Chairman indicated, on April 27, that the committee was drafting a bill that would mandate reporting for private companies that are victims of large-scale cyber breaches. Modernisation of energy grids and other critical industries have also been planned, through a new 100-day initiative, to protect against potentially damaging cyberattacks.[16] Further, on the diplomatic front, on April 20 the US Congress approved the "Cyber Diplomacy Act" that would set up a Bureau of International Cyberspace Policy in the State Department. The Bureau will be headed by an ambassador, who would create an international strategy to guide efforts by the United States to engage with other nations on cybersecurity issues and to set norms on responsible behaviour in cyberspace.[17]

The top cybersecurity leadership was also strengthened with the nomination of former Deputy Director of the National Security Agency (NSA), Chris Inglis, as the National Cybersecurity Director (NCD) on April 12. The NCD position was recommended by the Cyberspace Solarium Commission and created by the Fiscal Year 2021 National Defense Authorisation Act (NDAA) on Jan. 1.[18] The NCD would take the lead on coordinating cyber strategy and policy, cybersecurity compliance across the federal government and be the locus for

[15] https://www.wsj.com/articles/biden-signs-executive-order-targeting-harmful-foreign-activities-by-russian-government-11618490399?mod=article_inline
[16] https://www.securityweek.com/us-takes-steps-protect-electric-system-cyberattacks
[17] https://kinzinger.house.gov/news/documentsingle.aspx?DocumentID=402678
[18] Actions - H.R.6395 - 116th Congress (2019-2020): National Defense Authorization Act for Fiscal Year 2021 | Congress.gov | Library of Congress

collaborating with the private sector.[19] The NCD will complement and enhance efforts of the Deputy National Security Advisor for cyber and emerging technology at the US NSC. Another former senior counterterrorism and cybersecurity official at the NSA, Jen Easterly, has been nominated to lead the Cybersecurity and Infrastructure Security Agency (CISA) under the DHS. [20]

While the EU, NATO and other allies expressed their solidarity with the US response, on April 16 the Ministry of Foreign Affairs of the Russian Federation countered US sanctions by expelling ten U.S. diplomats and backlisting eight former and incumbent U.S. officials, including FBI Director Christopher A. Wray, Attorney General Merrick Garland and former CIA Director Robert J. Woolsey. The Russian government also stated that "not a single round of sanctions will go unanswered" and announced a number of counter measures to be introduced in the near future.[21]

Iran nuclear plant suffers blackout

A power failure caused by a deliberately planned cyber-attack on Iran's Natanz uranium enrichment site on April 11 possibly damaged several thousand centrifuges. Iranian officials called it an act of sabotage.[22] Israel publicly declined to confirm or deny any responsibility. The timing of the attack on the Natanz facility was significant as it took place when US Secretary of State Lloyd Austin was in Israel.

In response to the attack, on April 16 Iran declared that it had enriched uranium at 60% purity for the first time at the Pilot Fuel Enrichment Plant at Natanz, using advanced centrifuges. Enrichment closer to weapons grade of 90% purity will create a critical building block for a Iranian nuclear weapon. [23]

Contrary to apprehensions that the blackout would derail diplomatic efforts to salvage the 2015 nuclear deal, discussions were held on April 17 in Vienna. The discussion centred on determining sanctions to be lifted and the measures Iran has to take to rein in its nuclear programme. Participants included EU officials and representatives from Britain, China, France, Germany, Russia and Iran.[24]

[19] Cyberspace Solarium Commission - Report
[20] https://breakingdefense.com/2021/04/huge-step-forward-biden-taps-first-national-cyber-lead/?
[21] https://www.mid.ru/en/foreign_policy/news/-/asset_publisher
[22] Iran Vows to Increase Uranium Enrichment After Attack on Nuclear Site - The New York Times (nytimes.com)
[23] Reviving the Iran Nuclear Deal: What to Expect From the Talks and What Is at Stake - WSJ
[24] https://www.thehindu.com/news/international/envoys-to-iran-nuclear-talks-hail-progress-in-vienna/article34347520.ece

Investments on infrastructure and supply chain resilience

In his Joint Address to Congress on April 28, President Biden called for huge federal investments, including $2.3 trillion in infrastructure and $1.8 trillion in family and education programs.[25] Terming the infrastructure investments as necessary to compete with autocratic countries like China, he announced that the administration would spend $100 billion to "future-proof" broadband as part of an eight-year infrastructure plan, calling high-speed connections "the new electricity" necessary for all Americans. His infrastructure plan includes $50 billion for semiconductor research and manufacturing, another $50 billion to create an office at the Commerce Department focused on the country's industrial capacity, and support for the production of critical products. It also includes $50 billion for the National Science Foundation to create a technology directorate focused on semiconductors.[26] The package further includes $650 million in additional funding for the Cybersecurity and Infrastructure Security Agency (CISA) and $1 billion to update federal technology systems.[27]

Underscoring the importance of semiconductor chips as "infrastructure", on April 12 the US President convened a "virtual C.E.O. summit on semiconductor and supply chain resilience," with business executives of major digital and automobile companies. Biden stressed the need for innovation and investment in the semiconductor sector. [28]

On their part, global chip makers have ramped up their capital expenditure plans. Taiwan Semiconductor Manufacturing Co. plans to invest $100 billion over the next three years to boost production capacity, following Intel Corp.'s planned $20 billion on two new chip factories. TSMC, whose customers include Apple Inc and Qualcomm Inc, had already flagged a plan to spend of between $25 billion-$28 billion this year, to develop and produce advanced chips. Samsung previously earmarked about $116 billion by 2030 to further diversify its chip production, and is considering an investment of up to $17 billion to build a new facility in Austin, Texas. SK Hynix has approved a $106 billion project to build a new semiconductor complex in Yongin, about 50 kms south of Seoul, to ease supply shortages in the global market. However, all these companies face a "dilemma" to balance between China, their dominant market for exports, and the US, their security ally and the country holding the patents for manufacturing semiconductors.

[25] https://www.wsj.com/articles/bidens-joint-address-to-congress-key-takeaways
[26] https://www.nytimes.com/2021/04/12/business/semiconductor-chip-shortage.html?campaign
[27] AP April 04, 2021, 09:47 IST
[28] https://www.nytimes.com/2021/04/12/business/semiconductor-chip-shortage.html

EU Proposals for regulating Artificial Intelligence

EU has proposed a combination of the first-ever legal framework on AI and a new Coordinated Plan with Member States that addresses the human and societal risks associated with specific uses of AI, while strengthening AI uptake, investment and innovation across Europe. Announced on April 21, the bill would create a list of high-risk uses of AI that would be subject to new supervision and standards for their development and use. All remote biometric identification systems, such as facial recognition, are considered high risk and their live use in publicly accessible spaces for law enforcement purposes is prohibited in principle. Their use is subject to authorisation by a judicial or other independent body and to appropriate limits in time, geographic reach and the data bases searched. The Coordinated Plan outlines the necessary policy changes and investment at the Member States level.[29]The regulation would need to be approved by both the European Council, representing the bloc's 27 national governments, and the directly elected European Parliament.

While this is under active discussion, France announced on April 28 that it is planning to deploy Artificial Intelligence to broaden counter terror surveillance. The move to deploy algorithms and other technology to monitor the web-browsing of terror suspects comes as the French president comes under pressure to crack down on terrorism and Islamist separatism.[30]

China leads in Central Bank Digital Currencies

A January 2021, a report by the Bank of International Settlements declared that 86 percent of central banks worldwide are actively engaging in some form of Central bank digital currencies (CBDCs), and many are running digital currency pilots. It is not just U.S. adversaries who see the appeal of having an alternative to dollar-based, cross-border transactions; even some U.S. allies are looking for ways to undercut this leverage. China intends to use the combination of its digital yuan and strong electronic-payment platforms (such as Alipay and WeChat) to degrade the efficacy of U.S. sanctions and expand its influence for economic coercion.[31]

China is the world leader in the development of a CBDC, with 200 million yuan (US$30.4 million) already distributed in pilot projects across the country, including in cities like Shenzhen, Suzhou and Beijing. On April 1, Wang Xin,

[29] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682
[30] https://www.wsj.com/articles/frances-macron-seeks-broader-counterterror-surveillance
[31] https://www.foreignaffairs.com/articles/china/2020-05-20/could-chinas-digital-currency-unseat-dollar?

head of the People's Bank of China (PBOC) research bureau, announced that cross-border application is now feasible.[32]

In contrast to digital payment systems like credit cards, debit cards, or mobile wallets, exchanging digital currency involves a near real-time settlement process, as CBDCs are backed by sovereign currencies of nation states. Private cryptocurrencies, on the other hand, are issued by private players and are not backed by a central bank, so unlike CBDCs, there are no tangible assets backing their value. This makes private cryptocurrencies like Bitcoin highly volatile assets.[33]

India on its part has recently introduced "The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021" in the Indian Parliament in order to create a facilitative framework for creation of the official digital currency to be issued by the Reserve Bank of India. The Bill also seeks to prohibit all private cryptocurrencies in India. However, it allows for certain exceptions to promote the underlying technology of cryptocurrency and its uses.[34]

Chinese regulatory oversight on technology companies

On April 29, China's central bank and other regulators ordered 13 technology firms, including Tencent Holdings Ltd., Byte Dance Ltd., Meituan, Didi Chuxing Technology Co. and JD.com Inc., to adhere to much tighter regulation of their data and lending practices. The People's Bank of China listed a number of regulatory lapses by these companies, including offering banking and other financial services without license, inadequate corporate governance and engaging in unfair competition. All 13 firms were advised to conduct comprehensive "self-examination and rectification" of their businesses.[35]These developments follow within days of a record antitrust fine of $2.8 billion imposed on Alibaba Group Holding Ltd. for abusing its dominant position over rivals and merchants on its e-commerce platforms. [36]

[32] https://www.scmp.com/economy/china-economy/article/3128104/china-hong-kong-begin-testing-digital-yuan-beijing-ramps?
[33] Reuters April 26, 2021
[34] LOK SABHA (loksabhadocs.nic.in) Serial 12 (New Bills)
[35] https://www.wsj.com/articles/chinese-financial-regulators-summon-big-tech-firms-11619698257
[36] https://www.wsj.com/articles/alibaba-hit-with-record-2-8-billion-antitrust-fine-by-chinas-market-regulator-11618018830?mod=itp_wsj&mod=djemITP_h

Microsoft hack reveal prior reconnaissance and data mining

The cyber-attack on Microsoft email exchange servers in March this year had compromised more than 60,000 government, corporate and private email systems around the world. As on April 1, more than 90% of Microsoft's customers had patched their systems to address the vulnerabilities used in the attack. Investigators from Microsoft Corp. and the U.S. government suspect that state-sponsored Chinese hackers, dubbed Hafnium, had done prior reconnaissance to affect such an indiscriminate and far-reaching cyber-attack. The hackers mined troves of personal information stolen beforehand or scraped off social-media sites. Mining of this data led the hackers to the system data administrators' email account names, essential to break into their targets. Among the potential sources of the personal data is China's vast archive of likely billions of personal records stolen from innocuous big data sets, like super market or flight booking, residing in the cloud without jurisdictional accountability.

This highlights the lack of an internationally accepted framework governing storage and cross border flow of data, affecting the global economy and national security. China has adopted a techno-nationalist model that mandates government access to data generated in the country by dominating digital platforms including 5G telecommunications networks. Through the so-called Digital Silk Road and the broader Belt and Road Initiative, it is imposing its model of data governance and data repository. An internationally accepted framework should address the issues regarding privacy standards, anonymising data by use of emerging technologies, and promoting open flow of data that respects jurisdictional accountabilities.[37]

[37] https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age

International Cooperation

U.S.-Japan Competitiveness and Resilience (CoRe) Partnership

US President Joe Biden and Japanese Prime Minister Yoshihide Suga met in-person at the White House on April 16. The summit meeting concluded with the signing of an overarching U.S.-Japan Competitiveness and Resilience (CoRe) Partnership focussed on digital technologies, among other contemporary issues. These include development, testing, and deployment of secure networks and advanced ICT including 5G and next-generation mobile networks ("6G" or "Beyond 5G"); launching a Global Digital Connectivity Partnership to promote secure connectivity; promoting development of global standards; cooperating on supply chain resilience; and promoting research and development of critical technologies. For the 5G and beyond initiative, the United States has committed $2.5 billion and Japan has committed $2 billion.[38]

It would be interesting to follow this development to see if the partnership is extended to Quad members. On April 27, India, Japan and Australia formally launched the Supply Chain Resilience Initiative (SCRI) to build resilient supply chains in the Indo-Pacific region while in March, Australia, India, Japan, and the U.S. (the Quad) created a critical and emerging technology working group.[39]

Australia-India Cyber and Critical Technology Partnership

On April 21, Australia announced three cyber projects with India under the Australia-India Cyber and Critical Technology Partnership (AICCTP) Grant Programme providing USD 12.7 million over four years. The partnership is part of Australia's International Cyber and Critical Technology Engagement Strategy that sets the goal for a safe, secure and prosperous Australia, Indo-Pacific and the world. The projects include development of ethical frameworks and best practices for emerging quantum technologies; operationalising ethical frameworks in the critical technology supply chains of global companies; and addressing privacy and security challenges in next generation telecommunications networks.[40]

[38] Fact Sheet: U.S.-Japan Competitiveness and Resilience (CoRe) Partnership | The White House
[39] Fact Sheet: Quad Summit | The White House
[40] https://telecom.economictimes.indiatimes.com/news/australia-announces-cyber-projects-with-india-under-aicctp/82190758

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

www.delhipolicygroup.org