Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG Cyber Review

Volume 1, Issue 8

SEPTEMBER 2020

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. 1, Issue 8
September 2020

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

DPG Cyber Review is compiled by our research team from publicly available information and open source media to provide an overview of significant developments related to cyber and digital technology domains during the month. Your comments and feedback can be addressed to Brig. Abhimanyu Ghosh (Retd.), Senior Fellow for Cyber Security and Digital Technologies at abhi.ghosh@dpg.org.in

Cover Photographs:

Shri Ajit Doval, National Security Advisor, delivering keynote speech at virtual Cyber Conference COCONXIII-2020 on September 18, 2020 Source: YouTube

U.S. Secretary of State Mike Pompeo speaking at a news conference on the "Clean Network" program at the US State Department. Source: https://cdn.cfr.org/sites

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

DPG Cyber Review
Vol. 1, Issue 8
September 2020

Contents

Abstract

September 2020 started with the banning of an additional 118 Chinese apps by the Indian Government, bringing the total to 177, on grounds of national security. The decision was vindicated when the media reported, a few days later, that a Chinese tech company had monitored personal data of more than 10,000 Indian organisations and individuals, including political leaders and bureaucrats. Cyber-attacks were also reported from Chinese state sponsored hackers on Indian companies and Government networks. The US based China Aerospace Studies Institute (CASI) reported that China had carried out cyber-attacks on Indian satellite communications. However, the Indian Space Research Organisation (ISRO) maintained that its systems have not been compromised.

A draft cabinet note (DCN) on implementation of a national strategy on AI is under preparation. A report by the International Data Corporation (IDC) has predicted that India's Artificial Intelligence (AI) spending will grow from $300.7 million in 2019 to $880.5 million in 2023, at a compound annual growth rate (CAGR) of 30.8 per cent. The Indian Government is preparing to release a National Cyber-Security Strategy 2020 (NCSS 2020) which envisions a safe, secure, trusted, resilient and vibrant cyberspace for India's prosperity. The long awaited Personal Data Protection Bill (PDPB-2019) is likely to be placed before the Indian Parliament during its winter session.

In the global cyber space, a number of cyber attacks were reported. The month of September began with the hacking of the internal email system of the Norwegian parliament (Stortinget), while the month ended with a massive ransomware attack on more than 250 hospitals across the US. Tech companies are taking punitive actions against malign actors. Facebook removed three separate disinformation networks that targeted countries over geo-political issues.

Amidst the China-US tech war, both governments are taking proactive measures. The US State Department has announced a "Clean Network" Program, to rid the United States of Chinese technology and decouple the two economies in this sensitive sector. On September 4, President Donald Trump issued Space Policy Directive-5 on Cybersecurity Principles for Space Systems (SPD-5), the "nation's first comprehensive cybersecurity policy for space systems". The US imposed restrictions on exports to Semiconductor Manufacturing International Corporation (SMIC) of China. SMIC becomes the second leading Chinese technology company to face U.S. trade curbs after Huawei Technologies.

China announced a "Global Initiative on Data Security" to set global standards on data security, as a counter to these US initiatives.

The Pentagon is considering a program that would share its under-used military spectrum with private businesses, to spur innovation and counter Chinese domination of 5G devices and network equipment. The Pentagon is also stepping up military use of AI, in coordination with democratic allies.

China tested a prototype of the AR-500C unmanned aerial vehicle (UAV), a high-altitude drone helicopter, designed for missions on the country's disputed LAC with India.

September 2020 saw India entering into several agreements for Bilateral and Minilateral cooperation on Cyber security and digital technology innovation. Start-ups of India and Israel initiated a bilateral program to accelerate innovation and technology cooperation. India and Japan are joining hands in the technical development of 5G and 5G plus technologies with the help of other 'Quad' strategic dialogue partners. Officials of the four countries discussed the issue at a virtual meeting of the 'Quad' on September 25, 2020. Simultaneously, India, Israel, and the US have begun trilateral cooperation on digital leadership and innovation so that the three countries play a key role in delivering the next-generation 5G technology.

At the G-20 Trade and Investment Ministers' meet on September 22, India clarified that it is not in a position to accept uninhibited cross-border data flows.

National Developments

Cyber Threat Scenario

On September 2, the Government of India, invoking it's power under section 69A of the Information Technology Act, banned 118 additional Chinese apps, bringing the total number of Chinese apps banned by India since June, 2020 to 177. These apps were being used in stealing and transmitting users' data in an unauthorised manner to servers located outside India, which was prejudicial to sovereignty and integrity of India, the defence of India, the security of the state and public order. The ban is based upon a recommendation by the Indian Cyber Crime Coordination Centre (IC4) in the Ministry of Home Affairs.[1]

An investigative report in the Indian Express newspaper published on September 14, 2020 revealed that a Shenzen based Chinese tech firm, Zhenhua Data Information Technology Co. Limited, is actively monitoring more than 10,000 organisations and individuals in India, including top political leaders, key bureaucrats, scientists, journalists, actors, and industrialists, under a surveillance programme that has links to the Chinese Communist Party.[2]

An expert committee under the National Cyber Security Coordinator has been constituted on September 17, to study reports of the surveillance of Indian nationals by this Chinese firm, evaluate its implications and assess any violations of law. The Government of India has also taken up the matter with the Chinese side.[3]

On September 16, the US Justice Department indicted five Chinese nationals linked to China's Intelligence Service, who had infiltrated more than 100 companies and organisations, including the Indian government's networks, to steal intelligence and extort their victims. The conspirators conducted supply chain attacks that enabled them to embed malicious code in the software products of these companies. "In 2019, the conspirators compromised Government of India websites, as well as virtual private networks (VPN) and database servers supporting the Government of India", the indictment said.[4]

[1] https://pib.gov.in/PressReleasePage.aspx?PRID=1650669

[2] https://economictimes.indiatimes.com/news/defence/shenzhen-panopticon-the-whos-who-of-india-were-sitting-ducks-for-a-china-tech-company-reveals-

[3] https://www.wionews.com/world/snooping-row-china-says-zhenhua-has-no-links-to-the-government-it-is-a-private-company-328247

[4] https://ciso.economictimes.indiatimes.com/news/five-chinese-nationals-charged-in-mega-hacking-scheme-indian-govt-networks-hit-us/78159089

In a massive security breach, a malware attacked approximately 100 computers of the National Informatics Centre (NIC), it was revealed on September18, 2020. The computers at NIC's cyber hub contain crucial information and data on India's security, citizens and important government functionaries. A Special Cell of Delhi Police began an investigation into the matter under the Information Technology (IT) Act.[5]

Digital Technologies

A US-based China Aerospace Studies Institute (CASI) report released on September 23 claimed that between 2012 and 2018, China carried out multiple cyber-attacks on space systems, including Indian satellite communications, among other counter-space activities. However, the Indian Space Research Organisation (ISRO) maintains that its systems have not been compromised so far.

As per the report, China has multiple counter-space technologies, including ascent kinetic-kill vehicles (anti-satellite missiles), co-orbital satellites, directed-energy weapons, jammers, and other cyber capabilities, that are intended to threaten adversary space systems from the ground to geosynchronous orbit. One of the biggest weaknesses ubiquitous to all satellite systems is the use of long-range telemetry for communication with base stations, which can be compromised.[6]

Communication Technology

It was reported on September 20 that the Common Service Centre (CSC), an SPV under the Ministry of Electronics & Information Technology (MeitY), through its Village Level Entrepreneurs (VLEs), has undertaken the task of extending optical fibre connectivity to villages and gram panchayats or village blocks across India, under the Fibre to The Home (FTTH) or "Ghar Tak Fibre" initiative. In the coming 1000 days, every village of the nation will be connected with optical fibre.[7]

[5] https://ciso.economictimes.indiatimes.com/news/cyber-attack-on-nic-computers-email-traced-to-bengaluru/78187199

[6] https://www.timesnownews.com/india/article/china-attacked-india-s-satellite-communications-says-us-based-firm-report/656979

[7] https://telecom.economictimes.indiatimes.com/news/csc-undertakes-ghar-tak-fibre-initiative/78219583

The Minister of State for Communications, Sanjay Dhotre, informed Parliament on September 17 that more than 44 per cent of the mobile network equipment of state-run telco BSNL is sourced from Chinese firm ZTE and 9 per cent from Huawei. He said that there are comprehensive security conditions, including network audits from the security point of view, once in each financial year, as part of existing License Agreement for telecom service providers to address security concerns.[8]

5G Technology

At the 26th virtual meeting of the Asia-Pacific Tele community's wireless group (AWG) held from 14-18 September 2020, the Indian Department of Space (DoS) voiced its reservations to the allocation of 26 GHZ millimetre spectrum band for 5G services, saying it can cause interference between satellite and 5G mobile networks and impact quality of satellite coverage. Indian telecom companies, however, want that both the millimetre-wave spectrum and other 5G bands like 3.5 GHz are auctioned in India's first 5G spectrum sale, expected in 2021. They have warned that India will not be able to leverage the 5G global devices ecosystem, rapidly developing around the 26 GHz band, especially with US, China, South Korea and Japan backing 5G global deployments in this spectrum.[9]

Artificial Intelligence

Rao Inderjit Singh, the Minister for Planning, said in the Rajya Sabha on September 17, that the draft cabinet note (DCN) on implementation of a national strategy on AI is being steered by MeitY and is under consideration. NITI Aayog had released the draft National Strategy for Artificial Intelligence (NSAI) in June 2018, outlining proposed efforts in research, development, adoption and skilling in AI.

Major recommendations of the strategy include, inter alia, setting up of Centres of Research Excellence (CORE), focused on fundamental research, and International Centres on Transformational AI (ICTAI), focused on applied

[8] https://www.outlookindia.com/newsscroll/bsnls-44-pc-mobile-network-equipment-from-zte-9-pc-from-huawei/1937737

[9] https://telecom.economictimes.indiatimes.com/news/dept-of-space-dont-want-to-free-up-any-spectrum-in-26-ghz-mm-wave-telcos-fret/78237272

research. It is estimated that AI has the potential to add $957 billion to India's GDP and boost India's annual growth by 1.3 percentage points by 2035.[10]

As per an International Data Corporation (IDC) report titled "India Artificial Intelligence Market, 2020" released on September 30, 2020, India's Artificial Intelligence spending will grow from $300.7 million in 2019 to $880.5 million in 2023 at a compound annual growth rate (CAGR) of 30.8 per cent. A variety of industry-specific tech solutions supported by emerging technologies like the Internet of Things, Robotics, Blockchain, etc. are getting powered by complex AI algorithms and are cloud-enabled to reach their maximum potential. However, data trustworthiness and difficulty in selecting the right algorithm are some of the top challenges that hold organisations back from implementing AI technology.[11]

A study conducted by NASSCOM in association with EY on the subject "Can enterprise intelligence be created artificially? A survey of Indian enterprises", was released on September 3, 2020. It indicated that 74% of Indian enterprises have established a formal strategy to initiate or scale-up their AI programs while 78% believed re-skilling of the existing talent will aid in maximising value from their AI programs. Speaking at the report launch, Debjani Ghosh, President of NASSCOM, said that "As industry witnesses a rapid advancement in new technologies, Artificial Intelligence is increasingly becoming an imperative for businesses across industries. The NASSCOM - EY survey is a ready reckoner that enables business leaders to infuse technology at speed."[12]

Block Chain Technology

The Indian Government is reportedly planning to introduce a law to ban cryptocurrency trading, with the bill expected to be discussed shortly by the Union Cabinet before it is sent to parliament. The government will encourage blockchain, the technology underlying cryptocurrencies, but is reportedly not keen on cryptocurrency trading. It may be recalled that the Reserve Bank of India had in 2018 banned crypto transactions after a string of frauds in the

[10] https://economictimes.indiatimes.com/news/economy/policy/government-examining-national-strategy-on-artificial-intelligence-rao-inderjit-singh/articleshow/78163398.cms?from=mdr

[11] https://cio.economictimes.indiatimes.com/news/corporate-news/indias-artificial-intelligence-spending-grows-at-over-30-idc/78405440

[12] https://cio.economictimes.indiatimes.com/news/strategy-and-management/india-inc-continues-to-push-the-frontiers-of-technology-by-embracing-ai-survey/77906933

months following demonetisation. Cryptocurrency exchanges responded with a lawsuit in the Supreme Court and won a respite in March, 2020.[13]

Internet of Things

India Today magazine reported on September 23, 2020 that India is acquiring 30 General Atomics MQ-9B Guardian drones from the United States, in a deal valued at approximately $3 billion (Rs 22,000 crore). The MQ-9 is satellite-steered, can float above the target at 45,000 feet and stay on task for 35 hours. It can carry electro-optical/infra-red multi-mode radar and multi-mode maritime surveillance radar, laser designators, electronic support measures and various weapons packages. The Indian Navy has been made the lead service for this significant acquisition.[14]

[13] https://ciso.economictimes.indiatimes.com/news/government-plans-to-introduce-law-to-ban-cryptocurrency-trading/78138792

[14] https://www.indiatoday.in/india-today-insight/story/eye-on-china-a-3-billion-us-drone-acquisition-heads-for-mod-approval-1724393-2020-09-23

Government Initiatives

Strategy/Policy

National Security Adviser (NSA) Ajit Doval said on September 18 that the Indian Government is coming up with a National Cyber-Security Strategy 2020 which envisions a safe, secure, trusted, resilient and vibrant cyberspace for India's prosperity. The National Cyber Security Strategy 2020 will focus on all areas of cybersecurity through its three pillars- Secure (The National Cyberspace); Strengthen (Structures, People, Processes, Capabilities); and Synergise (Resources including Cooperation and Collaboration). Delivering a key-note address via video conferencing at a two-day virtual cyber conference 'Cocon 2020', Doval said that the government is striving hard to protect the country's cyberspace.[15]

On September 23, 2020 the Joint Committee of Parliament examining the Personal Data Protection Bill, 2019 (PDPB 2019) was granted extension up to the second week of the Winter Session of the Parliament, for the presentation of its report on the Bill. The panel has 20 members from the Lok Sabha and 10 from the Rajya Sabha. The Personal Data Protection Bill seeks to regulate the use of an individual's data by the government and private companies.[16]

The Telecommunication Regulatory Authority (TRAI) recommended on September 22 that the Department of Telecommunications (DOT) set up a multi-stakeholder body (MSB) to handle complaints about Net Neutrality and to frame guidelines for internet service providers. The body, to be set up as a nonprofit under the Societies Registration Act, 1860 would only have an advisory role, and the ultimate power to deal with Net Neutrality violations would rest with the DoT. Net Neutrality is the concept that all data over the internet should be treated the same way, with no selective slowing down, blocking, or discriminatory pricing for different content on the internet.[17]

Capability Building

Atal Innovation Mission (AIM) promoter NITI Aayog launched the Aatmanirbhar Bharat "ARISE-Atal New India Challenges" on September 9, to

[15] https://ciso.economictimes.indiatimes.com/news/centre-coming-up-with-national-cyber-security-strategy-2020-nsa-doval/78225856

[16] https://ciso.economictimes.indiatimes.com/news/joint-committee-of-parliament-on-personal-data-protection-bill-gets-extension/78285984

[17] https://www.medianama.com/2020/09/223-trai-advisory-body-net-neutrality/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+medianama+%28Medianama%3A+Digital+Media+In+India%29

spur applied research and innovation in Indian MSMEs and startups. The programme will be driven by the Indian Space Research Organization (ISRO); Ministry of Defence; Ministry of Food Processing Industries; Ministry of Health and Family Welfare; and Ministry of Housing and Urban Affairs, along with industries, to facilitate innovative solutions to sectoral problems. ISRO will adopt 100 Atal Tinkering Labs from the Atal Innovation Mission.

In the ARISE-ANIC (Applied Research and Innovation in Small Enterprises-Atal New India Challenges) programme, a total of 15 sector-specific challenges have been selected where three challenges have been allocated for each ministry. The ARISE-ANIC initiative will support deserving applied research–based innovations by providing funding support of up to Rs 50 lakh for the speedy development of the proposed technology solution and/or product.[18]

18 https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1652751#:~:text=ISRO%20and%20Four%20Ministries%20Roped%20In&text=Atal%20Innovation%20Mission%20(AIM)%2C,in%20Indian%20MSMEs%20and%20startups.

International Developments

Activities in global Cyber Space

On September 1, the Norwegian parliament (Stortinget) experienced a cyberattack on its internal email system, targeting the email accounts of elected representatives and employees, from which unspecified data were stolen.[19] Following the attack, the email service has been shut down to prevent further incursions and the Norwegian National Security Authority, Norway's intelligence agency, has launched an investigation.

Universal Health Services (UHS), a Fortune 500 hospital and healthcare services provider, has reportedly shut down systems at more than 250 hospitals around the US after a cyber-attack hit its network on September 27, 2020. The attack bears the sign of "RYUK" ransomware in which hackers hijack an organisation's systems, demanding a hefty ransom from victim. UHS operates over 400 healthcare facilities in the US and the UK, has more than 90,000 employees and provides healthcare services to approximately 3.5 million patients each year.[20]

It was reported on September 27, 2020 that the Microsoft Threat Intelligence Centre (MSTIC) has suspended 18 Azure Active Directory applications on its Cloud infrastructure that were being used as part of malicious command and control infrastructure by a China-based nation-state activity group, Gadolinium, that has been compromising targets for nearly a decade with a worldwide focus on the maritime and health industries. Gadolinium uses cloud services and open source tools to enhance weaponisation of their malware payload and to obfuscate detection.[21]

On September 24, Facebook removed three separate disinformation networks with links to the Russian military for violating its policy regarding Coordinated Inauthentic Behaviour (CIB). These networks had targeted several countries over geopolitical issues and regional politics. Although they did not directly target the upcoming US elections, these networks were linked to actors associated with US election interference in 2016.[22]

[19] https://www.cfr.org/blog/cyber-week-review-september-3-2020

[20] https://www.bleepingcomputer.com/news/security/uhs-hospitals-hit-by-reported-country-wide-ryuk-ransomware-attack/

[21] https://ciso.economictimes.indiatimes.com/news/microsoft-suspends-18-azure-accounts-tied-to-china-based-hackers/78343358

[22] https://about.fb.com/news/2020/09/removing-coordinated-inauthentic-behavior-russia/

On September 27, 2020 a US District Court Judge of the District of Columbia issued a temporary injunction on the ban on downloading the TikTok app from app stores. TikTok has more than 100 million active users in the US and about 700 million worldwide. The judge noted that the US government had "provided ample evidence that China presents a significant national security threat", but added that specific evidence that TikTok itself posed a risk and that taking its app off stores was required was "less substantial".[23]

On September 4, President Donald Trump issued a Space Policy Directive-5 on Cybersecurity Principles for Space Systems (SPD-5). The White House described SPD-5 as the "nation's first comprehensive cybersecurity policy for space systems." The policy responds to concerns that U.S. government and commercial space activities face cyber threats, such as hacking spacecraft guidance and control systems, "that can deny, degrade, or disrupt space operations, or even destroy satellites."

The US National Cyber Strategy, promulgated in September 2018, identified growing cyber-related threats to space assets and supporting infrastructure and committed the U.S. government to enhancing efforts to protect these from evolving cyber threats.[24]

Announcing a "Global Initiative on Data Security" on September 8, 2020 at a Beijing seminar on global digital governance, Chinese Foreign Minister Wang Yi cited growing risks to data security and what he characterised as efforts to politicise security issues and smear rival countries on technology matters. He added that the initiative aims to set global standards on data security, countering US efforts to persuade countries to ring fence their networks from Chinese technology. The initiative urges countries to oppose "mass surveillance against other states" and call on tech companies not to install "backdoors in their products and services to illegally obtain users' data, control or manipulate users' systems and devices."[25]

Digital Technologies

On September 25, 2020 the US government imposed restrictions on exports to Semiconductor Manufacturing International Corporation (SMIC), China's biggest silicon chip maker, after concluding there is an "unacceptable risk" that

[23] https://www.bbc.com/news/technology-54316992

[24] https://www.cfr.org/blog/white-house-adopts-cybersecurity-policy-activities-outer-space?utm_source=blognotification&utm_medium=email&utm_campaign=Blog%20Post%20Notification%20Net%20Politics&utm_term=NetPolitics

[25] https://www.reuters.com/article/us-china-usa-data/china-to-launch-initiative-to-set-global-data-security-rules-wsj-idUSKBN25Y1WK?il=0

equipment supplied to it could be used for military purposes. SMIC becomes the second leading Chinese technology company to face U.S. trade curbs after Huawei Technologies, whose access to high-end chips has been curtailed by its addition to the Entities List.[26]

On September 24, 2020 Taiwan President Tsai Ing-wen promised to help the island's key semiconductor industry, which is caught up in China-U.S. trade tensions. The world's biggest contract chipmaker, Taiwan Semiconductor Manufacturing Co Ltd (TSMC), is a major supplier to Apple Inc and Qualcomm Inc, as well as to Chinese firms like Huawei Technologies. China, on its part, is trying to nurture tech champions of its own, such as SMIC, its biggest chipmaker, and wean itself off reliance on U.S. suppliers.[27]

5G Technology

The US State Department has launched a "Clean Network" Program, to rid the United States of Chinese technology and decouple the two economies in this sensitive field. The program details the approach to 5G in five areas: Clean Network, Clean Storage, Clean Apps, Clean Cloud and Clean Undersea Cable. It is intended to protect the United States from national security threats, specifically from China. At its unveiling, the State Department announced a list of over thirty "clean countries" that had committed to excluding China from their 5G networks.[28] It may be recalled that the US President had signed a law creating a National Strategy to Secure 5G Implementation Plan in March, 2020.

On September 28, it was revealed that the Pentagon is considering a program that would share its under-used spectrum with private businesses to spur innovation. The sharing agreements would allow commercial use most of the time, but with the possibility of immediate pre-emption if the military needs the spectrum. The innovation and the investment that would follow in telecommunications will support the strategic goal of ensuring that the internet remains free from Chinese domination of 5G devices and network equipment.[29]

[26] https://telecom.economictimes.indiatimes.com/news/u-s-imposes-curbs-on-exports-to-chinas-top-chipmaker-smic/78336566

[27] https://in.reuters.com/article/taiwan-tech/caught-in-china-u-s-trade-war-taiwan-offers-support-to-chipmakers-idINKCN26F0JS

[28] https://www.cfr.org/blog/summer-ban

[29] By Heather Wilson Sept. 28, 2020 6:53 pm ET

Artificial Intelligence

The US Defense Secretary Dr. Mark T. Esper said at a virtual Joint Artificial Intelligence Center symposium on September 9, 2020 that the US will lead the world on the military use of artificial intelligence, including testing an AI pilot in a fighter by 2024. However, he added that America's AI will be governed by ethics that its great power rivals lack, and it will be coordinated with nearly a dozen democratic allies in a new "AI Partnership for Defence."[30] The race to develop AI is an important aspect of ongoing great power competition.

Internet of Things

China has tested a high-altitude drone helicopter designed for missions on the country's disputed LAC with India, according to its state media reports. A prototype of the AR-500C unmanned aerial vehicle (UAV) completed its maiden flight at an airport 4,411 metres (14,450 feet) above sea level in Sichuan province in southwestern China, neighbouring Tibet, on September 27, 2020. During the 15-minute flight, the Chinese-designed and built drone completed a series of tests including climbing, hovering and rotating before landing.[31]

The AR-500C is meant to be a reconnaissance and communication hub that can also serve as an electronic jammer, guide weapons fire, and detect nuclear radiation or chemical contamination. The test flight confirmed that the drone could carry a payload of 80kg (176lbs) and stay aloft for more than five hours. The state-owned Aviation Industry Corporation of China (AVIC) said on September 28 that the drone could deliver cargo to the high-altitude Tibetan Plateau.

[30] https://breakingdefense.com/2020/09/ai-will-dogfight-human-pilots-in-tests-by-2024-secdef/

[31] https://www.scmp.com/news/china/military/article/3103535/lift-chinas-high-altitude-helicopter-drone-prototype

International Cooperation

Bilateral/Minilateral Cooperation

A Memorandum of Understanding (MoU) was signed on September 22 between Israel's Start-Up Nation Central and India's International Centre for Entrepreneurship and Technology (iCreate), to initiate a bilateral program to accelerate innovation and technology cooperation between start-ups and corporates from both countries. "This MOU is an important step in realising the potential of the India-Israel relations in the field of innovative technologies," said Prof. Eugene Kandel, CEO of the Start-Up Nation Central.[32]

This agreement is an important milestone in the growing innovation collaboration between Israel and India, in line with the visions of the respective Prime Ministers. Israel has the most startups per capita worldwide, and India is the top innovation destination in Asia. Together, both countries continue to form partnerships and collaborations in technology and innovation to solve a range of global issues like Covid-19, renewable energy and more, and implementing high-end technologies including AI and Big Data Analysis.

Prime Minister Narendra Modi spoke to the newly appointed Japanese Prime Minister Yoshihide Suga on September 24, 2020 and decided to take the bilateral special strategic and global partnership to a new level. India and Japan are to join hands in technical development of 5G and 5G plus technologies with the help of other 'Quad' strategic dialogue partners - the US and Australia- and Israel. The development of next generation telecommunications technologies will be discussed between the 'Quad' Foreign Ministers in Japan on October 6, 2020.[33]

The US, India, Japan and Australia are exploring ways to evolve a common approach on 5G telecom technology, expanding their strategic cooperation under the framework of the 'Quad' which is primarily focused on the Indo-Pacific region. Officials of the four countries discussed the issue at a virtual meeting of the 'Quad' on September 25, 2020. Noting the importance of digital

[32] https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/israel-and-india-sign-mou-to-collaborate-in-tech-innovation-start-ups/articleshow/78258499.cms?from=mdr

[33] https://www.medianama.com/2020/09/223-india-japan-quad-cooperation-5g-tech-china/

connectivity and secure networks, the officials discussed ways to promote the use of trusted vendors, particularly for fifth generation (5G) networks.[34]

India, Israel and the US have initiated trilateral cooperation on digital leadership and innovation so that the three countries can play a key role in delivering the next-generation 5G technology in a way that is "open, interoperable, reliable and secure". "The collaboration in 5G is a first step towards bigger cooperation", said the United States Agency for International Development (USAID) Deputy Administrator, Bonnie Glick, to PTI after a US-India-Israel forum on strategic, tech and development/water cooperation discussion on September 4, 2020. Skill development, innovation and entrepreneurship, water and renewable energy cooperation will be other areas of this trilateral cooperation.[35]

India is also looking to play a bigger role along with its partners for setting global standards in the 3rd Generation Partnership Project (3GPP), a group of standards organisations which develops protocols for telecommunications. India has been successful in this global standards consortium to gain acceptance for the first Indian rural standard for telecommunication. It is understood that the majority of 3GPP standards thus far have been set by Chinese telecommunication development companies.[36]

Multilateral Cooperation

Speaking at the G-20 Trade and Investment Ministers' meet on September 22, 2020 Commerce and Industry Minister Piyush Goyal said that in view of the huge digital divide among countries, there is a need for policy space for developing countries to finalise laws governing digital trade and data. India is not in a position to accept the concept of Data Free Flow with Trust (DFFT), an initiative promoted by Japan. It goes against India's draft national e-commerce policy which has proposed regulating cross border data flows, locating computing facilities within India to ensure job creation and setting up a dedicated 'data authority' for issues related to sharing of community data.[37]

DFFT promotes uninhibited cross border flows of data and seeks to eliminate restrictions on cross-border transfer of information by electronic means,

[34] https://telecom.economictimes.indiatimes.com/news/quad-countries-deliberating-on-common-approach-on-5g-technology/78337793

[35] https://www.bbbnews.net/india-israel-us-collaborate-on-secure-5g-network-official/

[36] https://www.hindustantimes.com/india-news/india-and-japan-to-tie-up-for-5g-technologies-quad-to-pitch-in/story-AO6Rnv5JSjzuulS9WMgJ3L.html

[37] https://ciso.economictimes.indiatimes.com/news/india-not-in-position-to-accept-uninhibited-cross-border-data-flows-piyush-goyal/78266255

including personal information and the storing of data in foreign servers. The idea was proposed by Japan at the World Economic Forum's annual meeting last year.

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

www.delhipolicygroup.org