Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

JULY 2022

Volume III, Issue 7 | July 2022

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. III, Issue 7
July 2022

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. III, Issue 7
July 2022

Contents

Abstract

Adversarial threat actors from China, North Korea, Pakistan and Russia have been persistent in targeting India. While a Pakistani hacker group targeted Indian educational institutions, Russian malware was used for a cyber-attack on Oil India's (OIL) systems in Assam, with the hacker demanding a ransom of $75,00,000.

In the information space, Rutgers University in the US found evidence of a sharp rise in hate speech cases against Hindus on social media platforms, after a religious row. A new "Digital India Act" is in the offing to regulate "deliberate" misinformation and doxing as offences, as under the present Information Technology Act, 2000 there is no provision against spreading misinformation online.

Twitter filed a petition in an Indian Court seeking legal review of multiple notices issued to it by the Indian government to take down content, alleging "Disproportionate use of power" by officials to block content under Section 69 (A) of the Information Technology Act, 2000. The Indian government has contended that the notices were commensurate with its large user base, and the Twitter compliance rate is low for India as compared to other countries.

Starting July 26, a total of 72 GHz of 5G airwaves were auctioned by the Government of India, with participation from four entities — Reliance Jio, Bharti Airtel, Vodafone Idea and Adani Data Networks. A major decision taken by the Government regarding allotment of spectrum for private networks has spurred Indian companies to deploy indigenous technology stacks for 5G services locally, as well as exploring opportunities for taking their services to the world.

On the international front, the heads of the US FBI and Britain's MI5 jointly reaffirmed concerns about China's economic espionage to steal intellectual property and the Chinese government's efforts to stifle dissent abroad. Meanwhile, the Cyberspace Administration of China (CAC) fined ride-hailing company Didi Global $1.18 billion after a year-long probe that found the company breaking the country's data security and personal information protection laws. China faces a growing problem with data leaks because of its surveillance overreach to exercise social control.

The European Council has approved conclusions on foreign information manipulation and interference (FIMI), taking lessons from the ongoing Russia-Ukraine war. A bipartisan Bill was introduced in the US Senate seeking to

strengthen national security against quantum-computing threats. The US Senate passed a landmark $280 billion Industrial Policy Bill that aims to strengthen America's manufacturing and technological edge to counter China, particularly by incentivising production of semiconductors.

India has taken the lead in setting up a BIMSTEC cyber-response team by 2025 to deal with "real-time" information sharing on cyberattacks.

National Developments

Adversarial activities against Indian cyberspace

Over half of adversarial advanced persistent threat (APT) actor activities targeting India have originated from China, North Korea, Pakistan and Russian criminal groups. IBM's Threat Intelligence Report indicated that India was among the top three nations that experienced most server access and ransomware attacks in Asia in 2021.[1]

A CISCO TALOS report of July 14 revealed that a Pakistani advanced persistent threat (APT) group known as Transparent Tribe has been responsible for a new and ongoing phishing campaign targeting students at various educational institutions in India, at least since December 2021. Transparent Tribe has been circulating a compromised MS Word document, created in the name of a leading technology institute in India, to deceive targets.[2] Another phishing campaign has been targeting government websites across the world, including the Indian government's portal https://india.gov.in, extorting the affected users. Earlier, a Russian malware planted from a server in Nigeria was used for a cyber-attack on Oil India's (OIL) systems in Assam, with the hacker demanding $75,00,000. India has reported more than 670,000 such cyber security cases until June 2022.[3]

There is also a sharp rise in criminal activities in the Information space. On July 8, a release by the Ahmedabad Cyber Crime Branch identified Dragon Force of Malaysia and Hactivists of Garuda of Indonesia, who claimed to have hacked over 2000 Indian websites, leaking data of government departments and educational institutes. These groups initiated a cyber war against India and had appealed to Muslim hackers worldwide to "unite and start a campaign" against the country after recent religious controversies.[4] On July 13, Rutgers University in the US found evidence of a sharp rise in hate speech cases against Hindus on social media platforms. According to their analysis of 1 million tweets, Iranian trolls spread anti-Hindu stereotypes and memes to create division as part of their campaign to accuse the community of committing genocide on

[1] Cyber attacks: India among top 3 most-affected nations in Asia - The Statesman

[2] https://www.freepressjournal.in/mumbai/pakistan-backed-hacker-outfit-targets-indian-students-educational-institutions-report

[3] https://www.wionews.com/india-news/india-reports-more-than-670k-cyber-security-cases-until-june-499153

[4] Cyber war against India: Gujarat cops identify 2 hacker groups from Malaysia, Indonesia – ThePrint – PTIFeed

minorities. The research has shown a correlation between the "intensity of hate messaging over social media and the eruption of real-world acts of violence."[5]

As India is establishing itself on the global stage, there are constant attacks through misinformation, disinformation and false campaigns. On July 18, the Indian Prime Minister said that national defence is no longer confined to borders but has expanded towards space, cyberspace and the economic and social spheres. He highlighted the need for a 'whole-of-government approach" to combat myriad national security challenges.[6] The rising number of cyber security incidents is especially alarming since the country still does not have a National Cybersecurity Strategy or a data protection regulation in place.

New legislation in the offing to regulate misinformation and digital technologies

The IT Act 2000 is currently India's core legal framework that regulates social media platforms and e-commerce companies. Recognising that it lacks provisions for unique on-line offences, on July 13 the Indian Government announced that a new "Digital India Act" is under consideration to regulate "deliberate" misinformation and doxing as offences. Under the present IT laws, there is no provision against spreading misinformation online, which is seen only through the lens of defamation. Similarly, "doxing" is unique in the online sphere, and essentially attempts to publish private or identifying information about a particular individual on the internet, including social media profiles, publicly available data, government records, typically with malicious intent. The Digital India Act will also regulate net neutrality, online privacy, algorithmic accountability of social media platforms and new and emerging technologies such as blockchain and artificial intelligence.[7]

Twitter files petition in Court against Indian government orders

On July 5 the US micro-blogging site Twitter filed a petition in an Indian Court seeking legal review of multiple notices issued to it by the Indian government to take down content. Alleging "disproportionate use of power" by officials to block content under Section 69 (A) of the Information Technology Act, 2000, the company expressed concern about provisions that make the compliance officer personally liable in case of non-compliance. Twitter itself has issues

[5] US Research Finds Evidence of Sharp Rise in Hate Speech Cases Against Hindus on Social Media (news18.com)

[6] https://theprint.in/india/national-defence-no-longer-confined-to-borders-expanded-towards-cyber-social-space-pm-modi/1044460/

[7] https://indianexpress.com/article/technology/tech-news-technology/new-it-act-looks-to-rein-in-deliberate-misinformation-8027748/

with its own transparency mechanisms in content moderation decisions. Citing figures from Twitter's own global transparency data, a government review stated that during the first six months of 2021, 95% of the total legal demands directed at Twitter originated from five countries, namely Japan, Russia, Turkey, India, and South Korea and among these, Twitter's compliance rate in India was "abysmally low", at 11%.[8]

Section 69 (A) of the IT Act, 2000 allows the Centre to issue blocking orders to social media intermediaries "in the interest of sovereignty and integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognisable offence relating to above".[9]

5G Spectrum auction in India gets rolling

Starting July 26, a total of 72 GHz of airwaves were auctioned by the government, with participation from three telecom Service Providers (TSPs) and Adani Data Networks, which applied for 5G telecom spectrum auction that will not be in the consumer mobility space. The auction, with a validity period of 20 years, covered nine bands, including sub-GHz and mm Wave bands. The government's decision to slash the base price for the 700 MHz band by as much as 40% has been welcomed as the Sub-GHz spectrum will be important for providing 5G services in rural areas. With Reliance Jio being the sole bidder in this premium band, it will be better positioned to take 5G beyond urban areas and metros. The mid-band (3.3-3.67 GHz) and high-band (26 GHz) airwaves also attracted strong interest. The auction has been valued at over 1.49 trillion rupees ($18.6 billion), nearly double the government's initial estimates. Based on the auction results, the government will allocate the spectrum by August 14.[10]

An important decision pertaining to this auction has been regarding allotment of spectrum for private networks, which is being lapped up by technology companies for deploying technology stacks for 5G services, making India an innovation hub. On July 18, L&T Technology Services became the first technology company to publicly express interest in the government's direct allocation of spectrum for captive 5G networks. It will obtain spectrum to set up a 5G non-public network to build use cases on the technology for defence

[8] Twitter takedown orders proportional to user base: MeitY, IT Security News, ET CISO (indiatimes.com)

[9] Explained: Why Twitter has moved court against govt's content-blocking orders | Explained News,The Indian Express

[10] ashwini vaishnaw: Govt received bids worth Rs1.49 lakh crore in spectrum sale, auction may continue till Thursday: Ashwini Vaishnaw - The Economic Times (indiatimes.com)

purposes. On July 20, Japanese company Rakuten Mobile indicated that it is partnering with major technology companies like Microsoft, Google and Amazon to deploy its cloud based Open RAN solutions, keeping in mind the Indian market. The 5G auction will also throw open commercial business opportunities for global companies such as Ericsson, Samsung and Nokia to lay down the networks.[11]

Security of networks will be of utmost importance once 5G rolls out. Towards this end, on July 11 the Indian government ordered telecom businesses to only purchase devices from "trusted sources" for network expansion or upgrades, dealing a severe blow to Chinese telecom equipment manufacturers, including Huawei and ZTE, which have been unable to clear the stipulations of the National Security Directive on the Telecommunication Sector (NSDTS).[12]

India is however lagging much behind China, which continues its leadership position to innovate and develop 5G mobile technology. According to a report, China has deployed 916,000 5G base stations, accounting for 70% of the world's total, while the number of 5G-connected devices has now surpassed 365 million, accounting for 80 per cent of the global total.[13]

Indian industries step up chip manufacturing

It was reported on July 4 that the Vedanta Group expects its semiconductor business turnover to be in the range of $ 3 to 3.5 billion in the first phase by 2026-27, out of which around $ 1 billion will come from exports of both displays and semiconductor components. Vedanta Foxconn JV is among three companies that have applied for setting up semiconductor manufacturing units in the country.[14]

Vedanta will look at making 28 nanometer (nm) chipsets. The company has earmarked investments of up to $ 20 billion for semiconductor business, and it plans to invest $ 15 billion in the first 10 years.

[11] https://www.wsj.com/articles/india-telecom-companies-bid-heavily-in-first-5g-auction-11658932986

[12] https://dot.gov.in/sites/default/files/Brief%20on%20launch%20of%20Trusted%20Telecom%20Portal-1.pdf?download=1

[13] https://www.globaltimes.cn/page/202107/1228513.shtml

[14] https://www.business-standard.com/article/companies/vedanta-group-eyes-3-5-bn-turnover-from-chip-biz-one-third-from-exports-122070300440_1.html

The company expects to start manufacturing display units in 2024-25 and semiconductors by 2025-26. Last year Vedanta acquired Taiwan-based Avanstrate to enter into display fab manufacturing.[15]

Indian Air Force launches Centre of Excellence for AI

On July 10, Indian Air Force launched its Center of Excellence (COE) for Artificial Intelligence-UDAAN (Unit for Digitisation, Automation, Artificial Intelligence and Application Networking) in New Delhi. The Al center will handle all aspects of Analytics, Machine Learning, Natural Language Processing, Neural Networks and Deep Learning algorithms, in coordination with various PSUs, MSMEs and leading academia in the field of Artificial Intelligence.[16]

The AI COE with high-end computers and big data storage capabilities, coupled with full-spectrum Al software suites, will substantially enhance the operational capability of the IAF.

IIT Kanpur launches program for Cyber Physical Systems

On July 16, the C3iHub of IIT Kanpur Launched the second cohort of 14 startups under the Startup Incubation Program with the objective to foster the next generation of Cybersecurity Entrepreneurs. The startups were chosen from all domains of cybersecurity including UAV Security, Blockchain, Intrusion Detection, and Cyber Physical System.

The mission of C3iHub is to address cybersecurity issues in cyber-physical systems like critical infrastructure, automotives, and unmanned aerial vehicles (drones). In the cyber-physical system, cybersecurity is eventually linked with general areas of cybersecurity, including network security, cryptography, intrusion detection, and deception technology.[17]

[15] semiconductor manufacturing: Vedanta Group eyes $3.5 billion turnover from chip business, one-third from exports, Telecom News, ET Telecom (indiatimes.com)

[16] artificial intelligence: Indian Air Force launches its center of excellence for Artificial Intelligence in New Delhi, Government News, ET Government (indiatimes.com)

[17] https://indiaeducationdiary.in/c3ihub-iit-kanpur-launches-the-second-cohort-of-startups-with-the-objective-to-foster-the-next-generation-of-cybersecurity-entrepreneurs/

International Developments

Heads of FBI and MI5 Issue Joint Warning on Chinese espionage

On July 6, the heads of the US FBI and Britain's domestic security service-MI5 jointly reaffirmed concerns about economic espionage and hacking operations by China, as well as the Chinese government's efforts to stifle dissent abroad. The two Agencies issued warnings to business leaders about the threats posed by Chinese espionage to steal Intellectual Property. Last year, the Biden administration had publicly blamed Chinese state sponsored hackers for an attack on Microsoft's email system and had indicted 4 Chinese nationals. A separate notice was issued on July 6, warning state and local government leaders and business executives about Chinese efforts to influence policymaking through overt and covert means.[18]

The UK has also joined the US effort to limit Chinese equipment from next-generation telecommunications networks.

China has rejected the accusations by these countries as groundless[19]

Chinese GPS Tracker System found bugged

On July 20, cybersecurity researchers identified six severe vulnerabilities in the Chinese 'MiCODUS' GPS tracker, potentially allowing hackers to track individuals without their knowledge, remotely disable fleets of corporate supply and emergency vehicles, abruptly stop civilian vehicles on dangerous highways, and more. There are believed to be 1.5 million 'MiCODUS' devices, across 169 countries, in use by individual consumers, government agencies, militaries, law enforcement and corporations. GPS tracking devices such as these can greatly increase cyber risk and assist planned criminal activities.[20]

China slaps $1.18 bn fine on Didi Global over national security

On July 21, the Cyberspace Administration of China (CAC) fined ride-hailing company Didi Global $1.18 billion after a year-long probe that found the company breaking data security and personal information protection laws. Didi was found to have illegally processed nearly 12 million pieces of user photo information, 107 million entries of facial recognition data, 53.5 million entries

[18] Heads of FBI, MI5 Issue Joint Warning on Chinese Spying - WSJ

[19] https://www.securityweek.com/us-uk-leaders-raise-fresh-alarms-about-chinese-espionage

[20] gps: 6 bugs in popular Chinese GPS tracker put 1.5 mn vehicles at tracking risk, IT Security News, ET CISO (indiatimes.com)

of age data, 16.3 million entries of occupation data, and 1.4 million entries of data about family relations.

The Chinese authorities had initiated a cybersecurity probe into Didi after it launched a $4.4 billion IPO in New York in June last year.

To protect sensitive data, China's government has built one of the world's strictest cybersecurity and data-protection regimes. With crackdowns on Internet companies, China has also tightened mobile app development rules with stricter requirements for content and data protection.[21]

Despite those efforts, China has a problem with data leaks. A Wall Street Journal report of July 21 found a large Chinese database offered for sale in online cybercrime forums and Telegram communities. Four of the stolen caches contained data likely taken from government sources. One reason for such a massive data leak is China's surveillance state: the government's mass collection of personal information aids social control but can also become a vulnerability which undermines national security.[22]

EU Council approves Conclusions on FIMI

On July 18, The European Council approved Conclusions on foreign information manipulation and interference (FIMI), deriving lessons from the ongoing Russia-Ukraine War. The Conclusions underline how foreign information manipulation and interference is often used as part of broader hybrid campaigns and aims at misleading, deceiving and destabilising democratic societies, by creating and exploiting cultural and societal frictions in a strategic and coordinated manner.

The Conclusions affirm the EU's commitment to engage in multilateral formats with the United Nations and other international and regional organisations and call for well-defined measures that can be taken against FIMI actors to protect EU public order and security.[23]

[21] https://in.investing.com/news/china-slaps-118-bn-fine-on-ridehailing-major-didi-global-over-national-security-3282471

[22] https://www.wsj.com/articles/china-has-a-problem-with-data-leaks-one-reason-is-its-surveillance-state-11658410752

[23] Council Conclusions on Foreign Information Manipulation and Interference, 18 July 2022

Quantum Computing Cybersecurity Bill introduced in the US Senate

On July 25, a bipartisan Bill was introduced in the US Senate that seeks to strengthen national security against quantum-computing threats. The "Quantum Computing Cybersecurity Preparedness Act" addresses federal agencies' preparedness for quantum computing and strategies to migrate federal agencies' information technology systems to post-quantum cryptography.[24] These strategies would address the challenges posed by adversaries to steal standard cryptographic systems using the processing powers of Quantum computing. The Office of Management and Budget (OMB) will supervise the migration process. The OMB will also guide federal agencies for one year after the National Institute of Standards and Technology (NIST) issues post-quantum cryptography standards and will keep Congress informed on the status of federal agencies' migration to post-quantum cryptography standards and on post-quantum cryptography risks, defences and necessary funding. This bipartisan legislation will require the government to inventory its cryptographic systems, determine which are most at risk from quantum computing, and upgrade those systems accordingly.[25]

On July 12, the US National Institute of Standards and Technology (NIST) decided to standardise four "quantum-resistant" cryptographic algorithms that are meant to protect sensitive data from national security risks posed by quantum computers. The four encryption algorithms NIST selected will become part of their post-quantum cryptographic standard to be released in 2024. However, the Agency has advised organisations to start preparing for the transition immediately by following the Post-Quantum Cryptography Roadmap that suggests taking inventory of current cryptographic practices, creating a plan for the transition, and alerting the organisation's IT department of the upcoming transition. The Biden Administration has also issued a memorandum to address risks posed by quantum computers capable of cracking the Defense Department's encryption systems.[26]

Senate Passes $280 Billion Industrial Policy Bill to Counter China

On July 27, the US Senate passed a $280 billion Industrial Policy Bill aimed at building up America's manufacturing and technological edge to counter China. The Bill outlines a long-term strategy to address the nation's intensifying geopolitical rivalry with Beijing, by subsidising cutting-edge

[24] MIR22641 (senate.gov)

[25] https://www.securityweek.com/senators-introduce-bipartisan-quantum-computing-cybersecurity-bill

[26] NIST picks 4 'quantum-resistant' encryption algorithms to protect US data - Breaking Defense

technologies and innovations to bolster the nation's industrial, technological and military strength.[27]

Known as the CHIPS Plus package, the Bill also provides a large five-year investment in public R&D to increase America's competitiveness in the global supply chain. It would add $200 billion for scientific research, especially into artificial intelligence, robotics, quantum computing and a variety of other technologies. It further grants $10 billion to the Department of Commerce to provide subsidies to Chip manufacturing companies and to create 20 "regional technology hubs" across the country.[28]

On July 28, the US Congress passed the long-awaited CHIPS and Science Act, which aims to increase semiconductor manufacturing in the United States. CHIPS and Science Act provides $52.7 billion in funding for US computer chip makers and billions more in tax breaks to stimulate investment in manufacturing. Around $2 billion would go toward the Microelectronics Commons, a national network for onshore, university-based prototyping, lab-to-fab transition of semiconductor technologies, including Department of Defence-specific applications, and semiconductor workforce training.[29]

The US is not alone in implementing a policy of subsidies and state-backed investments. Governments in China, Europe and India, besides others, have taken up supply chain resilience as a critical policy and are making efforts to "onshore" semiconductor manufacturing. Japan's government will back TSMC to the tune of 476 billion yen ($3.5 billion) to build a factory there for the first time. The European CHIPS Act has a subsidy size of $46 Billion while the Indian Semi-Conductor Mission promises $30 Billion subsidies for Chips and technology supply chains with support of up to 50% of project cost. China on its part is directing a combined 1.5 trillion yuan ($221 billion) of public and private investments to replicate a Chips supply chain within its own borders.

A report by Nikkei Asia on July 27 observed that the so-called supply chain resilience is a myth, as no country is self-sufficient in the complex Chip manufacturing process. There are related dependencies on upstream supply chain for machineries, chemicals, natural gas, optical systems, valves, and several other components. The Wassenaar Arrangement, a multinational agreement signed by more than 40 nations to avoid such components being

[27] Senate Approves $280 Billion Bill to Boost U.S. Chip Making, Technology - WSJ

[28] https://www.news18.com/news/world/us-senate-passes-280-billion-bill-to-blunt-chinas-manufacturing-technological-edge-5645581.html

[29] https://www.news18.com/news/tech/us-congress-nod-to-chips-act-to-boost-semiconductor-production-pour-billions-in-fight-against-china-5648929.html

shipped to rogue states for military use, adds to further red tape. According to the Boston Consulting Group, "even a goal of reaching 70% to 80% self-reliance is "extremely challenging for any country or region to get all the fronts covered."[30]

On the regulatory front, it was reported on July 5 that the US is pushing the Netherlands to ban the Dutch company ASML from selling to China mainstream technology essential in making a large chunk of the world's chips. ASML is already banned from selling its most advanced equipment to Chinese firms, but the US is now trying to prevent ASML from selling older generation photolithography systems to China.[31]

ASML is the world's top maker of lithography machines that perform crucial functions to manufacture semiconductors. To frustrate US moves against China's technological advances, China is slated to build 31 major semiconductor fabs by 2024, as reported on July 24 by the chip-industry group SEMI. Western restrictions on China's access to advanced chipmaking machines have made China to bet big on basic Chips in its self-sufficiency push.[32]

[30] The resilience myth: Fatal flaws in the push to secure chip supply chains - Nikkei Asia
[31] Semiconductor Market: US Bans ASML From Selling Chipmaking Gear to China - Bloomberg
[32] China Chases Chip-Factory Dominance—and Global Clout - WSJ

International Cooperation

India takes the lead in setting up BIMSTEC cyber-response team

On July 15, a meeting of the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation's (BIMSTEC) cybersecurity expert group, organised by the National Security Council Secretariat (NSCS), was held in New Delhi. Delegates from Bangladesh, Bhutan, India, Myanmar, Nepal, Sri Lanka, and Thailand discussed plans to set up a BIMSTEC's computer emergency response team (CERT) by 2025 to deal with "real-time" information sharing on cyberattacks. The BIMSTEC Action Plan, to be implemented over five years, will cover exchange of information on cybersecurity, cybercrime, protection of critical information infrastructure, cyber incident response, and international developments related to cybersecurity norms. The Plan is slated to be finalised at the national security advisors' meeting in Myanmar later this year.[33]

Fourth India-Japan Cyber Dialogue

On June 30, the Fourth India-Japan Cyber Dialogue was hosted by India virtually in which both sides discussed important areas of bilateral cyber cooperation and reviewed the progress achieved in the areas of cybersecurity and Information and Communication Technologies (ICTs), including 5G Technology. The two sides exchanged views on latest developments in the cyber domain and cooperation during cyber consultations at the United Nations and other multilateral and regional fora.[34]

The US and Saudi Arabia Sign Bilateral Cybersecurity Agreements

On July 15, during President Biden's trip to Riyadh, the US signed two bilateral agreements on cybersecurity with Saudi Arabia's National Cybersecurity Authority – one involving the Federal Bureau of Investigation and the other the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Through these memoranda of cooperation, the US and Saudi Arabia will expand their existing bilateral relationship on this critical issue, share information about cybersecurity threats and activities of malicious actors to enhance shared defence and collaborate on best practices, technologies, tools, and on approaches to cybersecurity training and education.[35] Another memorandum of cooperation was signed between the two countries to

[33] Bimstec meeting: India takes the lead in setting up Bimstec cyber-response team - The Economic Times (indiatimes.com)
[34] https://www.mea.gov.in/press-releases.htm?dtl/35460/Fourth_IndiaJapan_Cyber_Dialogue
[35] FACT SHEET: Results of Bilateral Meeting Between the United States and the Kingdom of Saudi Arabia | The White House

advance deployment of 5G using open, virtualised, and cloud-based radio access networks and the development of 6G through similar technologies.

These cyber agreements are seen to be targeted at Iran, which has launched a range of cyberattacks, from website defacement and distributed denial-of-service attacks to espionage and ransomware attacks, against the two countries. The US has also entered into regional cyber collaborations with the UAE and Israel for sharing cyber threats and threat intelligence to deter and constrain Iran.[36]

***

[36] https://www.cfr.org/blog/cyber-week-review-july-29-2022

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

www.delhipolicygroup.org