Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

SEPTEMBER 2022

Volume III, Issue 9 | September 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 9
September 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 9
September 2022

Contents

Abstract i
National Developments 1
Bangladeshi Hacktivist group targets Indian government websites 1
"Trojan Virus" targets Indian Cyber Space 1
Draft Telecommunication Bill released for public consultation 2
5G ushers in digital transformation in India 2
TRAI interacts with stakeholders over satellite spectrum allocation 3
Major push to digital infrastructure development along LAC 4
India to graduate from being a Chip taker to a Chip Maker 4
International Developments 6
Iran hackers 'access database' with records of 9.5m Israelis 6
US DOJ sanctions Iranian hackers 6
US imposes Sanctions on Iran over Cyberattacks on NATO allies 6
Iranians offered Starlink service for communications amidst protests 7
Biden Issues Order to Block Chinese Investment in Technology 7
Twitter Ex-Security Chief testifies before the US Congress 7
EU Court of Justice Rules Against German Data localisation 8
Thailand and Vietnam become the top crypto-trading hubs 8
International Cooperation 10
Quad Foreign Ministers' Statement on Ransomware 10
IPEF nations resolve to stockpile emergency Chip supplies 10
India and Japan hold 2+2 Ministerial Meeting 11

Abstract

September saw further intrusions into Indian Cyber Space. A Bangladeshi hacktivist group "Mysterious Team Bangladesh (MT)", reportedly comprising students, has been targeting Indian government websites with Distributed Denial of Service (DDoS) attacks against domains and subdomains of several Indian state governments. CERT-In has also alerted the general public regarding proliferation of a new banking 'Trojan' virus that can encrypt an Android phone for ransom and is hard to uninstall.

A draft Indian Telecommunication Bill, 2022 along with a detailed explanatory note has been published for public consultation, seeking to streamline allocation of spectrum and amend provisions under the Universal Service Obligation Fund. The Bill enlarges the definition of telecommunication services, bringing Over-The-Top (OTT) services such as WhatsApp, Signal and Telegram, satellite-based communication services, Internet and broadband services, in-flight and maritime connectivity services, etc., under the ambit of the proposed law.

A recent Joint study by Deloitte and CII found that the low latency and high speed of 5G, coupled with the satellite internet broadband, can provide a significant convergence of the telecom ecosystem which will help to bridge the urban-rural divide. Local manufacturing of network equipment under the "Make in India" programme will also contribute to reforms and national security. Deployment of the 700 MHZ band is also expected to contribute to the goal of providing enhanced coverage.

The Telecom Regulatory Authority of India (TRAI) has started consultations with stakeholders, including the Department of Space (DoS) and Ministry of Information and Broadcasting (I&B), to seek views on allocation methodology of satellite spectrum.

India is expected to consume $80–90 billion of semiconductor chips by 2030, but at present it imports nearly 100 percent of its commercial semiconductor products. Thanks to the $10 billion incentive announced by the Government in December 2021, several conglomerates have decided to invest in domestic production of semiconductors. A Vedanta-Foxconn joint venture has announced an investment of $ 19.5 billion in India's first chip factory in Gujarat which will include a semiconductor fab unit, a display fab unit, and a semiconductor assembling and testing unit. Besides Vedanta, a consortium comprising Dubai-based NextOrbit and Israeli technology firm Tower Semiconductor has concluded a deal with the Karnataka government for a

plant in Mysuru, while Singapore-based IGSS Venture has chosen Tamil Nadu as the location for its semiconductor unit. Reportedly, the government is also open to investments in India by Chinese entities that offer technology and production capabilities to Apple Inc. in India, for which there is no alternative available.

The US has issued a license to "expand the range of internet services" available to Iranians, amidst massive protests in Iran following the custodial death of a female activist and restrictions placed by Iran on internet social media. This came in response to a request by Elon Musk for exemption of sanctions on Iran while offering the services of the satellite-internet system 'Starlink' to provide alternative communications to Iranians.

Twitter whistle-blower Peiter Zatko testified before the US Congress that the platform ignored security concerns in favour of financial incentives to executives to maximise profits. He alleged that the company was not properly tracking data access, required to respond to critical national security risks, including access gained by potential foreign agents.

Thailand and Vietnam have become the top crypto-trading hubs among the 10 members of the ASEAN. Beijing is leading the race among global central banks in the research and application of Central Bank Digital Currencies (CBDC), to move away from the dollar based financial system that is at the heart of all sanctions imposed by the US.

Foreign Ministers of the QUAD countries met in New York and committed to practical and result oriented cooperation to address the global threat of ransomware, which has been an obstacle to Indo-Pacific economic development. The meeting appreciated the progress made by the 36 countries supporting the U.S.-led Counter Ransomware Initiative (CRI).

14 member nations of the Indo-Pacific Economic Framework for Prosperity (IPEF), including India, met on September 8-9, and agreed to increase resiliency and investment in critical sectors and goods. The Group resolved to consider creating a formal system for sharing semiconductor devices, medical products, and other vital supplies during international emergencies. The IPEF joint statement includes the goal of establishing a crisis management mechanism for supply chains.

National Developments

Bangladeshi Hacktivist group targets Indian government websites

On September 22, an AI-powered cyber intelligence and threat detection company, Cloudsek, reported that a hacktivist group called "Mysterious Team Bangladesh (MT)" is targeting Indian government websites and servers.[1]

Distributed Denial of Service (DDoS) attacks were conducted against domains and subdomains of several state governments that include websites of Assam, Madhya Pradesh, Uttar Pradesh, Gujarat, Punjab, and Tamil Nadu. The attacks came to light when MT, with the handle "D4RK TSN", published a post on multiple platforms including Facebook, Pastebin, and Telegram, claiming to have conducted an HTTP flood DDoS attack on India-based government websites.

The group reportedly consists of students between the ages of 20 to 25 years that previously operated under hacker organisations like Elite Force 71, Bangladesh Cyber Anonymous Team, and Taskin Vau. These entities are predominantly motivated by hacktivism and have an association with the Indonesia-based "Hacktivist of Garuda". They also have a history of involvement in mass reporting of content across public platforms like Youtube, Facebook, Linkedin, etc.

"Trojan Virus" targets Indian Cyber Space

On September 15, CERT-In reported that Indian banking customers are being targeted by a new banking 'Trojan' virus -- SOVA -- which can stealthily encrypt an Android phone for ransom and is hard to uninstall. The advisory said that the malware can harvest usernames and passwords via key logging, stealing cookies and adding false overlays to a range of apps. Another key feature of the virus, according to the advisory, is the refactoring of its "protections" module, which aims to protect itself from different victim actions.

The agency said the malware is distributed via smishing (phishing via SMS) attacks, like most Android banking Trojans. SOVA was earlier focusing on countries like the US, Russia, and Spain, but in July 2022 it added several other countries, including India, to its list of targets.[2]

[1] https://www.communicationstoday.co.in/bangladeshi-hacktivist-group-targeting-indian-govt-websites/

[2] New mobile banking 'Trojan' virus prowling in Indian cyberspace, warns govt | Business Standard News (business-standard.com)

Draft Telecommunication Bill released for public consultation

On September 21 the draft of the Indian Telecommunication Bill 2022 along with a detailed explanatory note was published for public consultation and comments before October 20. As per the draft Bill, spectrum can be assigned through an auction or administrative process, based on requirements. It proposes penalties for a company if it fails to protect the interest of consumers or ensure fair competition. The mandate of the Universal Service Obligation Fund has been widened to include provisioning of telecom services to urban areas, R&D, skill development, and support of pilot projects.

The draft Bill brings Over-The-Top (OTT) services such as WhatsApp, Signal and Telegram, satellite-based communication services, Internet and broadband services, in-flight and maritime connectivity services, etc., within the enlarged definition of telecommunication services. In the event of war or national security concerns, the government can take over the control and management of, or suspend the operation of, any or all of telecommunication services. In the case of insolvency, spectrum assigned to an entity shall revert to government control.[3]

As the government is drawing up both telecom and IT laws afresh, it needs to decide which of the regulators — whether it is the Telecom Regulatory Authority of India (TRAI) or the proposed Data Protection Authority (DPA) under the forthcoming comprehensive Data Protection Bill — that will have oversight of these companies. Industry body COAI has termed the draft Indian Telecommunications Bill 2022 as "reformative".[4]

5G ushers in digital transformation in India

5G adoption can potentially change India's digital ecosystem radically. A joint report by Deloitte Touche Tohmatsu India LLP and CII titled 'Digital Reset – "Touching a Billion Indians" has examined how 5G can further the success stories of companies and regular consumers. The study found that thanks to 5G's high-speed and satellite broadband, there can be a significant convergence of the telecom ecosystem that will shape innumerable Indian lives by joining the urban-rural divide. Satcom will also enable massive machine type communication (mMTC) amongst Internet of Things (IoT) devices.

[3] https://dot.gov.in/relatedlinks/indian-telecommunication-bill-2022
[4] telecom bill: COAI terms draft telecom bill 'reformative', Telecom News, ET Telecom (indiatimes.com)

In an interview with The Print on September 9, the Director General of the Cellular Operators Association of India (COAI), a telecom industry body, indicated that thirteen Indian cities are gearing up for the rollout of 5G technology.[5] GOI has also come up with Private Partnership Models (PPP) to connect gram panchayats with internet across India. As 'Make in India' continues to gain momentum, the government is also promoting local manufacturing of network equipment by providing incentives to manufacturers.[6]

Reliance Jio has reportedly opted to deploy 5G network using standalone (SA) mode, while Bharti Airtel has chosen non-standalone (NSA) for 5G deployment citing ecosystem readiness. Reliance Jio is likely to spend Rs 800 billion, or 40% of its Rs 2 trillion planned 5G network Capex, on deploying 700MHz and 3.5GHz radio across 200,000 and 300,000 towers, respectively, according to the US-based venture capital firm Spark Capital. The 700 MHz band will enable it to offer better, stable, and faster connectivity in dense urban areas such as Delhi, Mumbai, Kolkata, etc.

The 700 MHz band for 5G has also seen deployment globally as well. TPG Telecom successfully rolled out its 5G standalone 700 MHz band services in Australia to provide coverage to 85% of Australia's population. KDDI (Japan) started its 5G 700 MHz rollout in March 2021, with the goal of providing an enhanced 5G experience by improving indoor and outdoor coverage. However, the most significant deployment in 2021 came from China, where China Broadcasting Network (CBN) and China Mobile are building out more than 480,000 5G base stations in the 700 MHz band. Nonetheless, rollouts on standalone mode account for only around 10% of all global 5G roll outs, mainly due to the lack of an ecosystem.[7]

TRAI interacts with stakeholders over satellite spectrum allocation

Promoting a self-sufficient space sector has been a priority of the government and a much-awaited space communication policy is likely soon. It was reported on September 17 that the Telecom Regulatory Authority of India (TRAI) is interacting with telecom and satellite players and officials in the Department of Telecommunications (DoT), the Department of Space (DoS) and the Ministry of Information and Broadcasting (I&B), to seek views on satellite spectrum and the allocation methodology for these airwaves in a run-up to a comprehensive

[5] 5G roll-out to start from these 13 cities in India; check if yours is in the list | The Financial Express

[6] https://www.ciiblog.in/digital-reset-touching-a-billion-indians/

[7] Reliance Jio: Jio may spend Rs 800 billion on deploying 700MHz, 3.5GHz radio for 5G: Report, Telecom News, ET Telecom (indiatimes.com)

consultation paper. So far, satellite spectrum, as in the KU/KA bands (12-18 GHz and 26.5- 40 GHz range), is being allocated administratively.

Bharti Global-backed OneWeb, Reliance Jio's JV with Luxembourg-based SES, Amazon's Project Kuiper, Viasat, Elon Musk's Starlink, and the Tata-Telesat combine are among those readying to enter India's broadband-from-space services segment. The TRAI consultations will help to resolve a clear divide among these players over allocation of spectrum for satellite communications, which are very useful for providing broadband services in remote, hilly, and inaccessible regions. This is also the only medium through which communications can be established in disaster zones when normal operations get affected.[8]

Major push to digital infrastructure development along LAC

According to media reports, the government is giving a major push to digital infrastructure development along the nearly 3,500 km long LAC. Each of the forward posts and Army units are being connected with optical fibre network and separate satellite terminals for bolstering overall surveillance and communications.

India to graduate from being a Chip taker to a Chip Maker

The Covid-19 pandemic and the Russia-Ukraine war have forced countries to become self-reliant in key strategic products like semiconductor chips. On September 13, a Vedanta-Foxconn Joint Venture announced an investment of ₹1.54 lakh crores ($ 19.5 billion) in India's first chip factory in the Indian state of Gujarat. The 60:40 joint venture will set up a semiconductor fab unit, a display fab unit, and a semiconductor assembling and testing unit on a 1000-acre site in the Ahmedabad district.[9] Besides Vedanta, a consortium comprising Dubai-based NextOrbit and Israeli tech firm Tower Semiconductor has signed a deal with the Karnataka government for a plant in Mysuru, while Singapore-based IGSS Venture has chosen Tamil Nadu as the location for its unit.

Even though India is expected to consume up to $80–90 billion of semiconductors by 2030, India imports nearly 100 percent of its commercial semiconductor products. India has thus far specialised in the R&D and design phases of the semiconductor supply chain. Despite its relatively strong R&D capabilities, India lags in semiconductor fabrication. It currently has only two

[8] reliance jio: Trai starts talks with stakeholders over satellite spectrum allocation, Telecom News, ET Telecom (indiatimes.com)
[9] Vedanta and Foxconn to build $19.5bn chip plant in India's Gujarat | Financial Times (ft.com)

fabs in the public sector: the Society for Integrated Circuit Technology and Applied Research (SITAR) in Bengaluru and the Semi-Conductor Laboratory (SCL) in Mohali. To correct the situation, India had announced an outlay of $10 billion to increase production of semiconductors in the private sector, which has resulted in the current bids for semiconductor manufacture.

The auction of 5G spectrum last month was accompanied with the allocation of spectrum for enterprises to set up non-public networks or private networks. On September 20, it was reported that the US Chip maker QUALCOMM, along with partners in its 5G Private Network Partner Ecosystem Program, is offering an end-to-end 5G Private Network solution, including chips for 5G RAN platforms. Further, it was reported on September 22, that the government is open to investments by Chinese entities that offer technology and production capabilities to Apple Inc. for which there is no alternative available.[10]

[10] apple china vendors: Government may let Apple's select China vendors set up plants in India - The Economic Times (indiatimes.com)

International Developments

Iran hackers 'access database' with records of 9.5m Israelis

The Israeli media reported on September 14 that an Iranian group of hackers "War Dark" had seized the data of 9.5 million Israelis, including Prime Minister Yair Lapid and opposition leader Benjamin Netanyahu. The group claims to have taken down the website of the Public Broadcasting Corporation Kan. The hackers released partial information on 8,300 records, which include, inter alia, names, identity cards, dates of birth and voting rights.[11]

US DOJ sanctions Iranian hackers

On September 14, the US Department of Justice announced an indictment against three Iranian hackers who used ransomware to extort a battered women's shelter and a power company. The trio had allegedly launched ransomware attacks on "hundreds" of victims, in Britain, Australia, Iran, Russia, and the United States, to extort money "largely" for their own accounts, and not for the Iranian government. A separate US Treasury announcement on the sanctions said the three were part of a larger hacking group tied to Iran's powerful Islamic Revolutionary Guard Corps (IRGC), and the US State Department has offered a $10 million reward for information on them.[12]

US imposes Sanctions on Iran over Cyberattacks on NATO allies

On September 9, the U.S. Treasury Department imposed sanctions against Iran's Ministry of Intelligence and Security (MOIS) and its Minister of Intelligence for engaging in cyber-enabled activities against the United States and its allies in NATO countries, including Albania. The announcement stated that the MOIS and its cyber actor proxies have conducted malicious cyber operations targeting a range of government and private-sector organizations around the world and across various critical infrastructure sectors, pointing to the disruptive cyberattacks that hit Albanian public services earlier this year. MOIS cyber actors were also responsible for the leaking of documents purported to be from the Albanian government and personal information associated with Albanian residents. The sanctions come after Albania cut diplomatic ties with Iran on September 7 over the July cyberattacks. NATO and

[11] Iran hackers 'access database' with records of 9.5m Israelis – Middle East Monitor
[12] Three Iranian Nationals Charged with Engaging in Computer Intrusions and Ransomware-Style Extortion Against U.S. Critical Infrastructure Providers | OPA | Department of Justice

the White House had issued statements condemning the ransomware and wiper attacks.[13]

Iranians offered Starlink service for communications amidst protests

Since Sept. 21, there have been massive protests across Iran following the death of a young activist Mahsa Amini in Tehran. To restore public order, the Iranian authorities restricted access of information to Iranians through WhatsApp and Instagram which affected most of its 80 million citizens. To counter official restrictions, Elon Musk sought an exemption to US sanctions on Iran to make his satellite-internet system Starlink available to Iranians. On September 23, the US Treasury Department issued a license to "expand the range of internet services available to Iranians" and help "the Iranian people be better equipped to counter the government's efforts to surveil and censor them." U.S. law gives the executive branch broad discretion over enforcing sanctions.[14]

Biden Issues Order to Block Chinese Investment in Technology

On September 15, the US President signed an executive order designed to sharpen the federal government's powers to block Chinese investment in technology in the United States and limit China's access to private data on US citizens. The new order is designed to focus the actions of the Committee on Foreign Investments in the United States (CFIUS) and reflects growing unease about China's ability to access the personal information that Americans hand over on mobile apps and other services.[15] CFIUS is in charge of blocking the foreign acquisition of American firms which might have a direct impact on national security. The most important element of the executive order directs CIFUS to consider whether a pending deal involves the purchase of a business with access to Americans' sensitive data, and whether a foreign company or government could exploit that information.

Twitter Ex-Security Chief testifies before the US Congress

On September 13, Twitter whistle-blower Peiter Zatko testified before the US Congress that the platform ignored security concerns in favour of company profits. He alleged that the executive team was financially incentivized to ignore root problems of employees having too much access to data. The Twitter leadership lacked competency to understand the scope of the problem and thus misled the public, regulators, and the company's own board, about its

[13] Albania Cuts Diplomatic Ties With Iran Over July Cyberattack | SecurityWeek.Com
[14] Elon Musk Has a Better Iran Idea.pdf
[15] Biden Issues New Order to Block Chinese Investment in Technology in the U.S. - The New York Times (nytimes.com)

lack of efforts to fight spam and foreign influence operations on its platform. He claimed that it was impossible for the company to respond to critical national security risks - including access gained by potential foreign agents.

The testimony is likely to affect the $44 billion takeover deal with Twitter from which Elon Musk is trying to exit. Zatko is also expected to meet with federal regulators, including the FTC, regarding data security concerns that could bring huge fines against Twitter.[16]

EU Court of Justice Rules Against German Data localisation

On September 20, the European Court of Justice (ECJ) ruled against a German law that mandated telecoms companies to retain customers' traffic data for 10 weeks and location data for four weeks. The stated aim of the law was to prosecute serious criminal offences or prevent specific risks to national security. Firms Telekom Deutschland and SpaceNet had challenged the law in German courts.

The case was heard in the European Court of Justice (ECJ) in Luxembourg, which ruled against the German legislation and opined that such measures were not permitted on a "preventative basis". "EU law precludes the general and indiscriminate retention of traffic and location data," the court said in a statement. However, it said that data can be retained in cases where an EU state faces a "serious threat to national security" that is "genuine and present", but such an instruction must be subject to review and can be retained only for a period deemed necessary.[17]

Thailand and Vietnam become the top crypto-trading hubs

Thailand and Vietnam have become the top crypto-trading hubs among the 10 members of the Association of Southeast Asian Nations (ASEAN). Thailand recorded $ 135.9 billion in crypto value transacted over the year, while Vietnam logged $ 112.6 billion in crypto buying and selling values from July 2021 to June 2022. Singapore booked $100.3 billion, as the city-state's financial regulator is in the process of drawing up rules to tighten scrutiny over retail trading of these tokens. On September 21, "Chain Analysis", a blockchain data platform, reported that users in lower-middle and upper-middle income countries often rely on

[16] Whistleblower: Twitter misled investors, FTC and underplayed spam issues - Washington Post

[17] EU Court Rules Against German Data Collection Law | SecurityWeek.Com

cryptocurrency to send remittances and preserve their savings in times of fiat currency volatility.[18]

Meanwhile, Beijing is leading the race among global central banks in research and application of Central Bank Digital Currencies (CBDC). The Digital Yuan is being promoted by China since May 2020, providing a way to bypass the US dollar. Digital money in China has been utilised in over 260m transactions valued at about 83bn yuan ($12bn) since its inception. Beijing reportedly hopes that the wider use of the digital Yuan will temper risks of financial decoupling if Washington moves to exclude China from the dollar system in the event of a war over Taiwan.[19]

[18] Thailand and Vietnam emerge as ASEAN crypto trading hot spots - Nikkei Asia - 'Nikkei Asia' News Summary (Japan) | BEAMSTART

[19] https://www.businesskhabar.com/money/finance/the-digital-yuan-offers-china-a-way-to-dodge-the-dollar/

International Cooperation

Quad Foreign Ministers' Statement on Ransomware

On September 23, the Foreign Ministers of Australia, India, and Japan and the Secretary of State of the United States, met in New York to commit to an open, secure, stable, accessible, and peaceful cyberspace. The Quad's Ministerial Group supported regional initiatives to enhance the capacity of countries to implement the UN Framework for Responsible State Behaviour in Cyberspace. The Ministers further committed to addressing the global threat of ransomware, which has been an obstacle to Indo-Pacific economic development and security, and appreciated the progress made by the 36 countries supporting the U.S.-led Counter Ransomware Initiative (CRI). They also supported regular, practical-oriented consultations against cybercrime in the Indo-Pacific region, to strengthen resilience, trust, and confidence in cyberspace, and effective incident-response capabilities. The Ministers underscored the importance of the multistakeholder approach and the role of the existing Global Forum on Cyber Expertise (GFCE) to build counter-ransomware capacity. They welcomed the negotiation of a possible new UN cybercrime convention as a long term means to address cybercrime more broadly which will have utility in countering ransomware.[20]

IPEF nations resolve to stockpile emergency Chip supplies

On September 8, 14 member nations of the Indo-Pacific Economic Framework for Prosperity (IPEF), including India – representing over 40% of the global economy – met at their first official in-person Ministerial meeting, to chart a path forward that will create economic opportunity, improve labour conditions, and promote sustainability for member nations' economies. At the conclusion of the Senior Officials' and Ministerial meetings, consensus ministerial statements were reached for each of the four IPEF pillars: Trade; Supply Chain; Clean Economy; and Fair Economy.[21][22]

Regarding Supply Chain resilience, the Ministers agreed to increase resiliency and investment in critical sectors and goods, establish an information sharing and crisis management response mechanism,

[20] https://www.mea.gov.in/bilateral-documents.htm?dtl/35749/Quad+Foreign+Ministers+Statement+on+Ransomware
[21] https://www.commerce.gov/sites/default/files/2022-09/Pillar-II-Ministerial-Statement.pdf
[22] https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/september/united-states-and-indo-pacific-economic-framework-partners-announce-negotiation-objectives

strengthen supply chain logistics and improve supply chain transparency. It was reported by Nikkei Asia that the member nations of the IPEF will consider creating a formal system for sharing semiconductor devices, medical products, and other vital supplies during international emergencies. IPEF countries would have mutual access to these stockpiles during events that disrupt supply chains, such as military conflicts and pandemics. This proposal responds to widespread reliance on China for many critical supplies, from industrially vital rare-earth elements to personal protective equipment (PPE) for health care workers. The IPEF joint statement includes the goal of establishing a crisis management mechanism for supply chains.[23]

India and Japan hold 2+2 Ministerial Meeting

On September 8, India and Japan held their 2+2 Ministerial Dialogue in Tokyo and reiterated the commitment of both countries towards deepening of bilateral security and defence cooperation and demonstrating the strength of Special Strategic and Global Partnership. The press statement at the conclusion of the 2+2 Dialogue reiterated the commitments of the two countries in promoting a rules-based order, ensuring respect for international law and norms, and safeguarding the global commons. Both countries welcomed deepened cooperation discussed through the Disarmament and Non-Proliferation Dialogue of February 2021, the Maritime Affairs Dialogue of September 2021, the Space Dialogue of November 2021, and the Cyber Dialogue of June 2022. Identifying some of the emerging technology areas in addition to conventional issues, both countries resolved to continue working on cyber security, 5G deployment, and critical and strategic minerals.[24]

***

[23] U.S.-led Indo-Pacific nations to consider emergency chip stockpile - Nikkei Asia

[24] https://www.mea.gov.in/bilateral-documents.htm?dtl/35684/Joint+Statement+Second+IndiaJapan+22+Foreign+and+Defence+Ministerial+Meeting

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

www.delhipolicygroup.org