Delhi Policy Group
Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

MARCH 2022

Volume III, Issue 3 | March 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 3
March 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

© 2022 by the Delhi Policy Group

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

DPG Cyber Review
Vol. III, Issue 3
March 2022

Contents

Abstract

The Russia-Ukraine War which has been ongoing since February 24 has not witnessed high-profile cyberattacks. However, social media platforms along with other electronic media have become dominant weapons for Information Warfare. India's dependence on western platforms, which have taken several partisan and unilateral actions, has impacted its cyber space during the war. This has brought to fore the need for "Atmanirbhar Internet" and self-reliance.

India's cyberspace continues to be plagued by cyber incidents, with more than 212000 cybersecurity incidents reported by the Indian Computer Emergency Response Team (CERT-In) in 2022. The growing expansion of India's cyber threat canvas is primarily dominated by persistent cyberattacks from Pakistan and China.

India has joined the European Union and nine other countries for fostering international cooperation to promote data protection and privacy standards across the Indo-Pacific region and Europe, with harmonised legal and policy frameworks for trans-border flows of data with trust. India's own data privacy law, in the making since 2019, is now set to get Parliament's approval by the monsoon session in 2022.

India's plans to roll out 5G by August 15 will be feasible only if the basic issues of Frequency Spectrum, Security testing of network equipment to identify "trusted products", indigenisation of hardware and software, and finally, infrastructure development are taken up in earnest.

On the international front, the Russian-Ukraine War has thrown up the challenges of massive dis-information campaigns and economic sanctions, providing opportunities to technology platforms to weaponise the internet and catalysing moves towards nation states adopting alternative governance frameworks. Innovative adoption of commercial technology and crowd sourcing by Ukraine has shown results against the asymmetric kinetic onslaught by Russia.

The Australian Government has pledged A$9.9 billion ($7.4 billion) for a Project named REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, and Enablers), that will significantly expand the Australian Signals Directorate's offensive cyber capabilities and defensive resilience to meet challenges from adversaries.

The US and the European Commission President announced an agreement on data privacy and trans-Atlantic data flows with trust and security to protect data of European citizens. The EU enacted a Digital Markets Act to protect citizens from large technology companies that collect data from different services to offer targeted advertisements without users' consent.

At the 14th India-Japan Annual Summit held in New Delhi, the two Prime Ministers reviewed areas of digital cooperation with a view to enhancing the digital economy.

The Quad Senior Cyber Group met in Sydney to review measures to expand cybersecurity cooperation and strengthen cyber resilience and critical infrastructure protection in the region. The meeting followed decisions taken by the Quad leaders at their summit on March 3.

National Developments

Russia-Ukraine war: Impact on India's Cyber space

In the ongoing Russia-Ukraine conflict, while there is near absence of cyberattacks that could alter the course of war, social media platforms along with electronic media have become dominant weapons for Information Warfare. Technology companies have implemented stringent policies suited to western interests, disregarding laws of nation states from which they earn sizeable revenue. India, like most countries dependent on western technology platforms, has been subjected to one sided bans and disinformation. Such technology restrictions have strengthened India's case for data localisation, national champions, resilient internet network architecture and a strong cyber security command centre. On March 23, the Indian Minister of State for Electronics and Information Technology called out big technology platforms of weaponising the internet and called for an "Atmanirbhar internet" to reduce dependence on services being provided by global firms. His comments came after YouTube blocked Indian news channel WION unilaterally over its coverage of the Russia-Ukraine war. In a deposition before the Delhi High Court on March 29, the government affirmed its commitment to safeguarding the fundamental rights enshrined in Article 14, 19 and 21 of the Constitution and emphasised that no social media intermediary guidelines, policy or actions can violate the constitutional rights of citizens.[1]

The weaponisation of financial sanctions has not only affected Russian banks and their subsidiaries but entities of other countries due to restrictions on the global SWIFT network. SWIFT is a high security "neutral financial network" used by 11000 financial institutions in 200 countries. This has prompted India and many other countries to consider frameworks independent of the digital payments system. India has already been pro-active in creating indigenous technology stacks, including the Universal Payment Interface (UPI) and global card payment network (RuPay). On March 30, it was reported that the Bank of Russia and the Reserve Bank of India are working on creating a new framework for trade and banking and working on a mechanism for the creation of a rupee-rouble exchange channel.[2]

To be self-reliant in the digital space, India needs to start with its own mobile operating system, bypassing the duopoly of western operating systems, and develop niche defence technology applications. With its huge technology

[1] social media: No social media intermediary can violate constitutional rights of citizens: IT Ministry sources, Telecom News, ET Telecom (indiatimes.com)

[2] https://economictimes.indiatimes.com/industry/banking/finance/banking/bank-of-russia-rbi-to-ready-framework-for-trade-banking/articleshow/90529279.cms

talent base, vibrant startup ecosystem, and government support, India is well placed to turn the Ukraine crisis into an opportunity for technology leadership.[3]

Cybersecurity Incidents continue unabated in 2022

On March 16, the Indian Parliament was informed that more than 212000 cybersecurity incidents were reported by the Indian Computer Emergency Response Team (CERT-In) so far in 2022, as compared to over 1402000 cyber security related incidents in 2021. While the origin of the attacks was not specified, previous attacks reportedly originated from Algeria, Brazil, China, France, Netherlands, North Korea, Pakistan, Russia, Serbia, South Korea, Taiwan, Thailand, Tunisia, USA and Vietnam.[4]

It was reported on March 19 that personal files and health records of at least 246000 personnel were hacked from the Central Industrial Security Force (CISF) database. This data in PDF files was available on the Raid Forums website on the Dark Web, and the hacker claimed that it was coming directly from a government CDN (content delivery network) server.[5]

This reflected the growing expansion of India's cyber threat canvas, primarily dominated by persistent cyberattacks from Pakistan and China. It was reported on March 17 that to thwart any attack on India's critical power infrastructure, a Computer Security Incident Response Team (CSIRT) is being set up. While the National Critical Information Infrastructure Protection Centre (NCIIPC) is the primary body that lays down guidelines for critical infrastructure, the new team will coordinate with NCIIPC and CERT-In (Indian Computer Emergency Response Team) to strengthen cybersecurity.[6] The government has initiated several such measures to safeguard critical installations across the country, but the process has been rather slow.

India joins international cooperation for data protection laws

On March 21, India joined the European Union and nine other countries for fostering international cooperation to promote data protection and privacy standards across the Indo-Pacific region and Europe. In a "Joint Declaration on Privacy and the Protection of Personal Data: Strengthening trust in the digital environment", the European Union, Australia, Comoros, India, Japan, Mauritius, New Zealand, South Korea, Singapore and Sri Lanka called for

[3] Rajeev Chandrasekhar: 'Big Tech weaponised internet amid conflict, presiding over splinter-net' | Business News,The Indian Express
[4] 3.94 Lakh Cybersecurity Incidents In 2019 As Per CERT Data: MeitY (inc42.com)
[5] Data of 2.46 lakh CISF personnel exposed online, IT Security News, ET CISO (indiatimes.com)
[6] India is assembling an ace team of cyber sleuths to protect its power grids (livemint.com)

comprehensive legal frameworks and policies covering both the private and public sectors, to meet the challenges of privacy and the protection of personal data, in view of rapid technological developments. The joint vision underlined core principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, limited data retention, data security, accountability and enforceable rights of individuals.[7]

India's own privacy Law still awaited

It was reported on March 13 that India will soon roll out a data protection framework, in the making since 2019, that will strike the right balance between protecting data, preserving privacy and enabling the business environment. The Joint Parliamentary Committee on Personal Data Privacy Bill 2019 (PDPB) tabled its report in both the Houses of Parliament in December 2021. However, industry and civil society remain sceptical on certain contentious issues. The government hopes to resolve these issues and pass the legislation by the monsoon session in 2022.[8]

Status report on 5G roll out

It has been appreciated that the 5G trials are proceeding vigorously across the country, in spite of differences among major telecom and satellite players regarding the spectrum allocation. The auction and allocation of various frequency bands are tentatively scheduled in the second quarter of 2022. On March 25, the Parliament was informed that the spectrum auctions will be conducted soon, and the next-generation 5G services are expected to commence by August 15. The telecom regulator TRAI will shortly give its recommendations related to the upcoming auction.[9] However, there are certain issues needing immediate attention of industry and policy makers.

On March 10, the National Cyber Security Coordinator (NCSC) said that 5G will create new security challenges with complex software defined networks, necessitating security across the network. To counter the network security threats, the government has undertaken the initiative to implement the National Security Directive on the telecom sector (NSDTS). Security testing of devices, prior to certification, is being done under the Mandatory Testing &

[7] Joint Declaration by India, the European Union, Australia, Comoros, Japan, Mauritius, New Zealand, the Republic of Korea, Singapore, Sri Lanka on privacy and the protection of personal data: Strengthe (mea.gov.in)

[8] rajeev chandrasekhar: ETSA2021: India will draw up data laws to ensure business growth, privacy, says Rajeev Chandrasekhar - The Economic Times (indiatimes.com)

[9] 5G auctions: Spectrum auction to be conducted soon; 5G service to be launched by year end: Govt in RS, Telecom News, ET Telecom (indiatimes.com)

Certification of Telecom Equipment (MTCTE) regime, by the nodal Department of Telecommunication.

Several global and Indian device manufacturers including Samsung, Ericsson, Nokia, Cisco, Tejas Networks and HFCL have got the “trusted source” approval from India's NCSC, the designated certification authority. Some of the devices have also received the "trusted products" approval.[10] There is, however, a need for vendor diversity. In the oligopolistic market of 5G, there are only a few European and Chinese companies which dominate.[11]

To ensure security, attention is required for early deployment of “Make in India” network equipment. The initiative for Production Linked Incentive (PLI) has also been taken up by many device vendors. It was reported on March 24 that Samsung has applied for phase 2 of the PLI scheme for network equipment to locally manufacture 4G and 5G products. Earlier, Samsung had been importing the network equipment through the free trade agreement (FTA) route from South Korea and Vietnam. Samsung recently relocated its mobile and IT display production unit from China to India and is investing Rs 4,825 crore ($660.96 million) for the same.[12]

Another aspect of focus needs to be infrastructure building, which includes the fiberisation of sites and building adequate number of towers. At least 70% of towers need to be fiberised, from the current level of 33%, for the launch of 5G services. Compared to India, in South Korea 65-70% of sites have been fiberised, while in the US, Japan and China, the level of fiberisation is 80-90%. On March 28, it was reported that while fiberisation is ideal, backhaul infrastructure could also be built upon radio frequencies in the 7GHz to 40GHz bands, in addition to the V-band (60GHz) and the E-band (70/80GHz band). All these would require heavy investment, policy interventions and concerted efforts by the industry.[13]

[10] Samsung gets trusted source approval from India's NCSC, Telecom News, ET Telecom (indiatimes.com)

[11] Open Ran 5g: 5G requires uniform focus on security throughout network: Lt. Gen. Rajesh Pant, Telecom News, ET Telecom (indiatimes.com)

[12] Reliance Jio: Samsung plans to locally manufacture 4G, 5G gear; in talks with Jio, Airtel, Telecom News, ET Telecom (indiatimes.com)

[13] 5G auctions: 5G knocking on doors but where is the infrastructure?, Telecom News, ET Telecom (indiatimes.com)

International Developments

Asymmetric Warfare in Ukraine

Contrary to expectations, the use of cyber warfare in the Russian war with Ukraine has so far been limited. To date, the only significant, sophisticated operations with suspected Russian involvement are the attacks on the Viasat's satellite networks, attempts to install data-wiping malware on Ukrainian government systems, and attacks against two major Ukrainian telecommunications firms. Missiles and other stand-off weapon systems offer a faster and more effective means of achieving strategic objectives.

However, this could also be due to effective Ukrainian cyber defence, backed by technology and support from NATO. The people of Ukraine have also adopted unconventional use of commercial technology, including citizen-empowering social networks and crowdsourcing, to even out the asymmetry of kinetic war arsenals. A media report of March 28 suggested that Ukraine is using $2,000 commercial octocopter drones, modified with thermal imagers and antitank grenades, to find and attack Russian tanks at night. Ukraine's Aerorozvidka, its aerial reconnaissance team, has 50 squads of drone pilots who operate on commercial internet connections. In the face of cyberattacks on satellite internet communications on Viasat terminals, Elon Musk and his firm SpaceX have donated thousands of Starlink satellite internet-access terminals to Ukraine, including to the Aerorozvidka squads, with a relatively small cost of $499 each and $99 a month for service. The "IT Army of Ukraine", with approximately 400,000 volunteers, is employing the Telegram channel to coordinate digital attacks on Russian military digital systems. This digital flash mob has taken down Russian websites, blocked the +7-country code for Russia and eventually took down 3G services that Russia uses for secure connections.

Ukraine also has taken advantage of crowdsourcing. Civilians and Territorial Defence volunteers message coordinates of Russian tanks via the Viber social-messaging app, for the Army to bring down fire. On the flip side, uncoordinated employment of technology has given away their own location, which may be the reason for targeted Russian attacks on a mall or a theatre. All the same, Ukraine has become the symbol of asymmetric power of pervasive inexpensive commercial technology.[14]

India is also known for such innovative use of technology which will surely be tested during any future geo-political crisis. For the present, India's

[14] Ukraine's Asymmetric War - WSJ

dependence on western/Chinese technology platforms for email, social media and cloud computing needs a thorough review.

Western agencies probe cyber-attack on satellite internet

On March 19, Britain and the United States warned organisations of the risks associated with satellite communications, following the reported cyberattack coinciding with the Russian attack on Ukraine, disrupting broadband satellite internet access to more than 9,000 subscribers in Ukraine and elsewhere in Europe. The hackers had disabled modems that communicate with Viasat Inc's KA-SAT satellite, which supplies internet access to a significant number of subscribers in Germany, France, Hungary, Greece, Italy and Poland besides Ukraine.

This is seen as one of the most significant war time cyberattacks, because Viasat acts as a defence contractor for both the United States and multiple allies. It was reported by Reuters on March 11 that KA-SAT has provided internet connectivity to Ukrainian military and police units. Knocking out satellite internet connectivity could handicap Ukraine's ability to combat Russian forces.

Western intelligence agencies, including the U.S. National Security Agency, French government cybersecurity organisation ANSSI, and Ukrainian intelligence, are assessing whether the remote sabotage of the Viasat satellite internet communication was the work of Russian-state backed hackers. The cyber security firm Mandiant has also been requisitioned by Viasat for investigation.[15]

Responding to the cyberattack, SpaceX had promptly provided Starlink satellite resources, as already mentioned. However, on March 5 Starlink satellites were also reportedly jammed “near conflict areas”. Elon Musk, the founder of SpaceX, indicated in a series of tweets that SpaceX will bypass the jamming by software updates and reprioritised cyber defence.[16]

Impact of sanctions in the global digital space

In response to Russia’s aggression in Ukraine, massive sanctions have been imposed on it by the US, the EU and Japan, among other Western nations. This has impacted several aspects of the digital supply chain. On March 4, Microsoft

[15] https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/

[16] https://spacenews.com/spacex-shifts-resources-to-cybersecurity-to-address-starlink-jamming/

Corp, Apple Inc, Nike and Dell Technologies, severed connections with Russia. Companies have also moved to restrict Russian state-controlled media including RT and Sputnik. Facebook-owner Meta Platforms Inc and Alphabet Inc's Google and YouTube have also taken measures to restrict Russian state media from making money from advertisements on their platforms. On March 5, Mastercard and Visa suspended operations in Russia, affecting digital transactions through cards issued by Russian banks from working in other countries and block people with cards issued elsewhere from purchasing goods and services from companies in Russia.[17]

The US has repeatedly warned of cyberattacks from Russia in retaliation against sanctions and expressed concern that the Russian cyber security firm Kaspersky could be compelled to assist Moscow to intercept communications transiting Russian networks. On March 25, the US Federal Communications Commission (FCC) added Kaspersky along with China Mobile International USA and China Telecom (Americas) to the list of entities that pose an "unacceptable risk to US national security".[18]

On March 30, the US National Security Council reportedly discussed sanctioning Kaspersky Lab but the US administration remains divided on the issue, partly as the company's software is used by hundreds of millions of customers across the world, making it difficult to enforce sanctions. Kaspersky Lab has repeatedly denied that it works with the Russian or any government to facilitate cyber espionage or other malicious cyber activity. The alleged relationship between Kaspersky Lab and the Russian state is considered similar to how U.S.-based cyber firms cooperate with U.S. intelligence agencies.[19]

Australia Pledges $7.4B to Cyber-warfare

On March 29, the Australian Government announced A$9.9 billion ($7.4 billion) in budgetary funding for boosting intelligence and cybersecurity against the backdrop of increasing cyber warfare capabilities of adversaries such as Russia and China. The major share of the funding is for a Project named REDSPICE (Resilience, Effects, Defence, Space, Intelligence, Cyber, and Enablers) that will significantly expand the Australian Signals Directorate's offensive cyber capabilities, as well as the agency's ability to prevent hacking and other digital attacks. The government will also establish a new Cyber and Critical

[17] Mastercard and Visa Suspend Operations in Russia - The New York Times (nytimes.com)
[18] kaspersky: US bans Russian cyber company Kaspersky, firm calls move political, IT Security News, ET CISO (indiatimes.com)
[19] Proposal to Sanction Russian Cybersecurity Firm Over Ukraine Invasion Splits Biden Administration - WSJ

Technology Infrastructure Centre within the Office of National Intelligence. The project will create new positions, equipment and training.[20]

US and EU reach political agreement on Data Privacy

On March 25, the US President and the European Commission President announced an agreement on data privacy and trans-Atlantic data flows. Two earlier agreements for storing European data on US soil were deemed illegal by the EU's top court in 2015 and 2020, on the grounds that the U.S. didn't provide EU citizens effective means to challenge U.S. government surveillance of their data. The agreement will allow EU authorities "to once again authorise trans-Atlantic data flows that help facilitate $7.1 trillion in economic relations with the EU". While groups hailed the announcement, civil society activists in Europe believe that the agreement will not stand legal scrutiny like the earlier two agreements - "Privacy Shield" and "Safe Harbour" - unless it is coupled with changes to U.S. surveillance laws.[21]

Europe passes Digital Markets Act

The EU had pioneered the General Data Protection Regulation (EU GDPR) to protect people's online privacy in 2018. On March 24, the EU passed a Digital Markets Act, potentially bringing technology companies under new oversight similar to health care, transportation and banking industries. The law addresses the power of big tech companies, which will no longer be able to collect data from different services to offer targeted ads without users' consent. The EU is also expected to promulgate another law that would force social media companies such as Meta, the owner of Facebook and Instagram, to police their platforms more aggressively.[22]

On March 18, the US Justice Department endorsed legislation, akin to the EU law, forbidding large digital platforms such as Amazon and Google from favouring their own products and services over competitors, marking the first such support of antitrust measures. No new federal laws have so far been passed in the US to address unchecked powers of technology.[23]

Russia-Ukraine war prompts adversaries to move Courts

On March 21, a Russian court ruled that Meta, which owns Facebook, Instagram and WhatsApp, is an "extremist organisation" and banned it from operating on

[20] Australia Pledges $7.4 Billion to Cyberwarfare in Defense Boost - BNN Bloomberg
[21] U.S., EU Reach Preliminary Deal on Data Privacy - WSJ
[22] E.U. Takes Aim at Big Tech's Power With Landmark Digital Act - The New York Times (nytimes.com)
[23] Antitrust Bill Targeting Amazon, Google, Apple Gets Support From DOJ - WSJ

Russia's territory. The "extremist" label will apply to Instagram and Facebook, but not to WhatsApp, and is effective immediately. Meta is the first commercial entity to be labelled an "extremist organisation" by Russia. Previously, the label was reserved for nongovernmental organisations, and religious or political groups. The Russian government's lawsuit against Meta was based on the company's decision to allow users in some countries to call for violence against members of Russia's military. Such actions are "aimed at inciting hatred and hostility toward citizens of the Russian Federation," the Russian prosecutor general's office said in a statement on March 11.

Earlier this month, Russia had passed another law that could effectively punish intentional spreading of "fake" news with as much as 15 years in prison. Several Western media organisations moved on March 4 to suspend their journalistic operations in Russia in response. The BBC said it would use shortwave radio frequencies to broadcast news in Kyiv and in parts of Russia.[24]

On March 24, the US government formally charged four Russian hackers said to be working with a government intelligence agency over a series of Cyberattacks that targeted energy firms around the world between 2012 and 2018. The criminals reportedly targeted hundreds of companies and organisations across approximately 135 countries. The indictment alleges that the criminals hacked into organisations in the energy sector, including oil and gas firms, nuclear power plants, and utility and power transmission companies, in an effort to gain persistent access to networks and SCADA systems.[25]

[24] russia ukraine war: Several Western news organisations suspend operations in Russia following censorship law - The Economic Times (indiatimes.com)

[25] Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide | OPA | Department of Justice

International Cooperation

14th India-Japan Annual Summit

India and Japan enjoy multi-faceted cooperation within the ambit of their 'Special Strategic and Global Partnership'. The Prime Ministers of both countries met in New Delhi for the 14th India-Japan Annual Summit on March 19. Their discussions covered several areas of digital cooperation and the "India-Japan Digital Partnership" with a view to enhancing the digital economy through promotion of joint projects for digital transformation. Welcoming the signing of a Memorandum of Cooperation (MoC) in the fields of Cybersecurity and ICT, they appreciated progress in the bilateral relationship in the cyber domain. They endorsed further cooperate in technology fields like 5G, Open RAN, Telecom Network Security, submarine cable systems, and Quantum Communications, and looked forward to greater cooperation among IT professionals. They also reaffirmed their commitment to the Quad Principles on Technology Design, Development, Governance, and Use, to be further shared by all like-minded nations.[26]

India-Australia Virtual Summit

The Prime Ministers of India and Australia met for the second India-Australia Virtual Summit on March 21, 2022. They welcomed the inaugural India-Australia Foreign Ministers' Cyber Framework Dialogue held on February 12 and cooperation on cyber governance, cyber security, capacity building, cybercrime, digital economy, and critical and emerging technologies. They reaffirmed their commitment to an open, secure, free, accessible, stable, peaceful and interoperable cyberspace and technologies that adhere to international law. They also welcomed the agreement to establish the India-Australia Centre of Excellence for Critical and Emerging Technology Policy in Bengaluru.[27]

Second India- Indonesia Security Dialogue

On March 17, India's National Security Advisor co-chaired the second India-Indonesia Security Dialogue (IISD) with Indonesia's Coordinating Minister of Political, Legal and Security Affairs to discuss cooperation in counter terrorism, maritime, defence, and cyber security domains. They signed an MoU for a

[26] India-Japan Summit Joint Statement Partnership for a Peaceful, Stable and Prosperous Post-COVID World (mea.gov.in)

[27] JOINT STATEMENT : INDIA-AUSTRALIA VIRTUAL SUMMIT (mea.gov.in)

Security Dialogue (IISD) that will enhance cooperation between the two countries on political and security issues.[28]

QUAD Senior Officials Meet to Strengthen Cyber Security

The Quad Senior Cyber Group met in Sydney on March 25 and held discussions on ways to expand cybersecurity cooperation and strengthen cyber resilience and critical infrastructure protection in the Indo-Pacific. India was represented by the National Cyber Security Coordinator. The Group recognised the need for improving cybersecurity in an increasingly digital world with sophisticated cyber threats. The meeting resulted in a work plan for further collaboration between Quad members, and with partners and industry in the region, to address common challenges. The group will report back to leaders through the established Quad processes.[29]

***

[28] Second India- Indonesia Security Dialogue (mea.gov.in)

[29] Statement by National Security Council Spokesperson Emily Horne on Quad Senior Cyber Group Meeting | The White House

DPG

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

www.delhipolicygroup.org