Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

OCTOBER 2020

Volume I, Issue 9 | October 2020

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

Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG Cyber Review
Vol. 1, Issue 9
October 2020

ABOUT US

Founded in 1994, the Delhi Policy Group (DPG) is among India's oldest think tanks with its primary focus on strategic and international issues of critical national interest. DPG is a non-partisan institution and is independently funded by a non-profit Trust. Over past decades, DPG has established itself in both domestic and international circles and is widely recognised today among the top security think tanks of India and of Asia's major powers.

Since 2016, in keeping with India's increasing global profile, DPG has expanded its focus areas to include India's regional and global role and its policies in the Indo-Pacific. In a realist environment, DPG remains mindful of the need to align India's ambitions with matching strategies and capabilities, from diplomatic initiatives to security policy and military modernisation.

At a time of disruptive change in the global order, DPG aims to deliver research based, relevant, reliable and realist policy perspectives to an actively engaged public, both at home and abroad. DPG is deeply committed to the growth of India's national power and purpose, the security and prosperity of the people of India and India's contributions to the global public good. We remain firmly anchored within these foundational principles which have defined DPG since its inception.

DPG Cyber Review

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

Cover 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. 1, Issue 9
October 2020

Contents

Abstract

India continues to be a target of unabated cyber-attacks by Pakistan and China. Important attacks included Dr. Reddy's Lab and the Press Trust of India. Frequency of the cyberattacks highlight the need to strengthen digital infrastructure and tighten cyber security control measures across all sectors in the country.

Month also saw the enunciation of new space policy that will open up the space sector to private Indian entities, encourage foreign direct investment and allow foreign companies to set up facilities for space related activities.

In the telecom sector there is growing understanding of the centrality of backbone infrastructure in particular spectrum allocation and fiberisation of towers as crucial to the rollout of 5G. Furthermore, in adoption of standards for 5G networks, there is a need to balance between the home-grown national standards and widely accepted international standards.

On the use of artificial intelligence (AI), Prime Minister Narendra Modi, while inaugurating the global virtual summit on artificial intelligence (AI), "Responsible AI for Social Empowerment (RAISE 2020)" on October 5, highlighted how the AI can empower India, while cautioning about the possible weaponisation of AI technologies by non-state actors.

Rational spectrum allocation is crucial for the growth of communication technologies. Towards this the government has constituted a Committee of secretaries (COS) to streamline the spectrum allocation process that will give a clear road map for the deployment of next generation networks.

On the international front, the semiconductor industry in the US is witnessing consolidation with new mergers and acquisitions. On October 27, Advanced Micro Devices Inc. (AMD) announced the plans to buy rival chip maker Xilinx Inc. in a $35 billion deal. In another development the U.S. National Security Council, on October 13, issued "National Strategy for Critical and Emerging Technologies (C&ET)", that aims at ensuring the United States, its allies and partners, continue to be the world leader in C&ET.

To further boost bilateral cooperation between India and Japan in the field of cybersecurity, information and communication technologies (ICT), Indian cabinet approved the signing of the Memorandums of Cooperation (MoC) which is likely to be signed at the India – Japan Summit later this year. To address the issue of communications security the members of the intelligence-

sharing "The Five Eyes" alliance, together with Japan and India, urged the ICT industry to address concerns of communications with end to end encryption that prevents legal access to the content by Law Enforcement Authorities.

National Developments

Cyber Threat Scenario

A Pakistan-backed hacker group, known as the 'Transparent Tribe', has been targeting Indian defence forces in a bid to steal critical infrastructure and strategic data by sending phishing emails. These hackers are reportedly being backed by China to gather intelligence against India.[1]

On October 22, Dr. Reddy's Lab, the Indian pharmaceuticals company, suffered a massive cyberattack that triggered a shutdown of its key facilities, in UK, US, India, Brazil and Russia. The attackers employed the "Ragnarok Cry" ransomware. Importantly, Dr. Reddy's Lab and the Russian Direct Investment Fund (RDIF), had recently entered into a partnership to conduct clinical trials of Sputnik V vaccine and its subsequent distribution in India.[2]

Similarly, the news agency Press Trust of India (PTI) suffered a ransomware attack on October 24, disrupting operations and the delivery of news. The ransomware was identified as "Lock Bit" that encrypts data and applications.[3]

The Indian government issued a warning to the micro-blogging website, Twitter, over misrepresentation of the country's map. The company was categorically instructed that any attempt to disrespect the sovereignty and integrity of India, which is also reflected in the maps, is totally unacceptable and unlawful.[4]

Data Security

The Joint Committee of Parliament on the "Personal Data Protection Bill, 2019 (PDPB-2019)", is currently interacting with major technology companies to look into concerns of data privacy and data security. Representatives of Facebook, Twitter, Amazon, Google and Paytm have already deposed before

[1] https://www.sundayguardianlive.com/news/pak-based-hackers-targeting-indian-defence-units-officials

[2] https://economictimes.indiatimes.com/prime/technology-and-startups/markets-shrugged-why-ignoring-a-cyberattack-on-dr-reddys-a-nifty-50-company...

[3] https://ciso.economictimes.indiatimes.com/news/massive-ransomware-attack-hits-pti-services-resume/78872937

[4] https://www.timesnownews.com/india/article/unacceptable-and-unlawful-india-warns-twitter-for-showing-leh-and-jk-in-china/671155

the panel. [5] India's personal data protection law will boost the growth of country's digital economy, by ensuring personal data privacy and security.

Digital Technologies

Space Technology

In a major and far reaching development that will provide a boost to Indian space sector, the Indian Space Research Organisation (ISRO) has decided to open its facilities to the private sector for its future projects on planetary exploration and outer space travel. The new policy will provide private companies a level playing field in satellite launches and space-based activities. The newly created Indian National Space Promotion and Authorisation Centre (IN-SPACe), has been tasked to put relevant mechanisms in place.[6]

It is expected that the induction of private sector in space research and activities will encourage foreign direct investment and allow foreign companies to set up facilities for making satellites, launch vehicles, ground stations and use spaceports among others.[7]

Communication Technology

Cellular Operators' Association of India (COAI) Director General SP Kochhar said on October 13,that the advent of 5G means that the telecom sector is now a force-multiplier for other sectors, and the government needs to view it as an "essential service provider" and enabler for industries, like water and electricity.[8]

In this regard rational spectrum allocation is seen as crucial for the growth of communication sector. The Telecom Regulatory Authority of India (TRAI) had, in November 2015, recommended that both E-band (between 57-64 GHz) and V-band (71-76 and 81-86 GHz) of spectrum should be allocated and not auctioned, for faster broadband rollout in the country. However, this has become a bone of contention between the telecom and the internet service providers.

[5] https://ciso.economictimes.indiatimes.com/news/parliamentary-panel-on-data-protection-bill-summons-jio-airtel-uber-ola-truecaller/78944714

[6] https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1663527

[7] https://www.communicationstoday.co.in/india-to-allow-foreign-companies-too-to-make-and-launch-satellites/

[8] https://telecom.economictimes.indiatimes.com/news/telecom-a-force-multiplier-for-all-sectors-should-be-seen-as-essential-service-enabler-coai-dg/78659941

The Broadband India Forum (BIF), which represents internet and technology companies, has recommended delicensing E and V frequency bands to unleash the full potential of these bands and proliferation of short-range devices (SRD).[9] Telecom companies, however, favour auction of these bands.

5G Technology

Adoption of standards for the growth of 5G is crucial. Reliance Jio has backed the country-specific 5G norm proposed by the Telecom Standards Development Society, India (TSDSI) that calls for the deployment of 5G services in the 3.4 GHz band and suggests mobile towers be spaced 12 km apart. However, Bharti Airtel and Vodafone Idea have recommended global standards recommended by the 3rd Generation Partnership Project (3GPP). 3GPP's 5G standard backs 5G deployment in the 700 MHz band and requies mobile towers to be spaced 6 km apart. 3GPP standards govern networks operations worldwide and has been backed by the International Telecom Union (ITU).[10] Varying standards may lead to inter operability challenges.

Fiberisation is another critical aspect for the growth of 5G, because of the backhaul requirement of microwave or wireless and optical fiber cable.[11]The National Digital Communications Policy 2018 had set a target of at least 60% tower fiberisation by 2022.[12] However, as of now just 30% of mobile towers have fibre-enabled backhaul. In terms of fibre to the home (FTTH) penetration, India has only 1.3 million FTTH households in comparison to over 350 million in China. The investments in fiberisation of the 5G networks is expected to be upwards of US$30 billion.[13]

Artificial Intelligence

Inaugurating a five-day global virtual summit on artificial intelligence (AI), "Responsible AI for Social Empowerment (RAISE 2020)" on October 5, Prime Minister Narendra Modi highlighted how the use of AI can empower India. He highlighted how the "National Programme on Artificial Intelligence" will be dedicated towards rightful use of AI for solving problems of society with trust

[9] https://www-financialexpress-com.cdn.ampproject.org/c/s/www.financialexpress.com/opinion/spectrum-of-change-unleashing-v-band-potential/2116040/lite/

[10] https://telecom.economictimes.indiatimes.com/news/telcos-differ-on-adoption-of-india-centric-5g-norms-bharti-airtel-vodafone-idea-caution-of-gaps-in-standards/78713787

[11] https://telecom.economictimes.indiatimes.com/news/5g-is-very-much-dependent-on-fiberization-airtel-cto-randeep-sekhon/78444072

[12] National Digital Communications Policy 2018, page 6

[13] https://techwireasia.com/2020/10/whats-holding-a-5g-roll-out-back-in-india/

and accountability. Algorithm transparency will be the key. He however warned against the weaponisation of AI by non-state actors.[14]

PM Narendra Modi Inaugurated a five-day global virtual Summit on AI-RAISE 2020 on October 5, 2020. Source: (PTI)

In a supporting development, the Chip-making giant Intel, on October 19, launched an Artificial Intelligence (AI) research centre in Hyderabad (INAI) in collaboration with the Telangana government, the International Institute of Information Technology-Hyderabad and the Public Health Foundation of India. INAI is an initiative to apply AI in solving population scale problems in the Indian context.[15]

Quantum Technology

Quantum cryptography and quantum key distribution will play a big future role in preventing major security breaches and overcoming application failures in AI. In an interview on October 11, the CTO of QNu Labs revealed that its quantum encryption, that could prevent future cyber-attacks by encrypting keys using quantum physics principles, has been deployed across Indian critical sectors including defence, telecom, banking and finance.[16]

[14] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1661885

[15] https://www.expresscomputer.in/artificial-intelligence-ai/intels-hyderabad-ai-centre-to-focus-on-road-safety-health/64921/?utm_source=newslettter&utm_medium=newsletter&utm_campaign=19102020

[16] https://analyticsindiamag.com/indian-firms-need-quantum-secure-key-distribution-to-prevent-future-attacks-says-cto-of-qnu-labs/

QNu lab is the first company to represent Indian quantum technology ecosystem globally at the Quantum Alliance Initiative (QAI), that has developed a set of recommended global standards for Quantum Key Distribution (QKD) and Quantum Random Number Generator (QRNG) technologies.[17] In an associated development the technology company Honeywell introduced its next-generation quantum computer, the System Model H1, in Bengaluru, on October 29, 2020. The H1 generation of computer, offers 10 fully connected qubits, a proven quantum volume of 128 and qubit reuse.[18]

Furthermore the allocation of ₹8,000 crores towards the development of Quantum Cryptography and Quantum Communication technologies, announced during the Union Budget 2020 will help India make significant strides in this space.

[17] https://www.insidequantumtechnology.com/news/quantum-alliance-initiative-develops-standards-quantum-key-distribution-quantum-random-number-generator-technologies/

[18] https://cio.economictimes.indiatimes.com/news/corporate-news/honeywell-introduces-next-gen-quantum-computer-with-10-qubits/78964278

National Initiatives

Strategy/Policy

A Committee of Secretaries (COS) has been constituted to streamline the spectrum allocation process for commercial use. In its meeting on October 14, 2020, the COS discussed ways to resolve spectrum frequency issues between the Department of Telecommunication (DOT) and other ministries. The COS has also been tasked to examine the roadmap for auctioning 5G Spectrum in the 26 GHZ Band, E-band and V-band to roll out latest technologies, optimise networks and ensure quality of service.[19]

Budgetary Support

The National Policy on Electronics 2019 envisions positioning India as a global hub for Electronics System Design and Manufacturing (ESDM) by focusing on size, scale, promoting exports and enhancing domestic value addition.[20]

Ministry of Electronics and Information Technology (MeitY) on October 6, approved 16 proposals under the Production Linked Incentive Scheme (PLI) for large scale electronics manufacturing, that extends an incentive of 4% to 6% on incremental sales of goods under target segments that are manufactured in India to eligible companies, for a period of five years subsequent to the base year (FY2019-20). The objective is to build a strong indigenous ecosystem across the value chain and integrate the same with the global value chains. This has elicited encouraging responses from the global as well as domestic mobile phone companies and electronic components manufacturers.[21]

Capability Building

India is set to achieve self-reliance in supercomputing through manufacturing of critical components in India.[22] In a virtual ceremony held on October 12, the Centre for Development of Advanced Computing(C-DAC) under the Ministry of Electronics and Information Technology (MeitY) approved partnership with the premier academic and R&D institutions of India for establishing supercomputing infrastructure and manufacturing of critical components as part of the National Supercomputing Mission in India. The Mission is

[19] https://telecom.economictimes.indiatimes.com/news/government-sets-up-a-panel-of-secretaries-to-streamline-telecom-spectrum-allocation/78652021

[20] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1662096

[21] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1662096

[22] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1663672

implemented and steered jointly by the Department of Science and Technology (DST) and MeitY.[23]

The Indian Army on October 29, launched the "Secure Application for Internet" (SAI), App, which is similar to WhatsApp, Telegram etc, and supports end-to-end secure voice, text and video calling services for Android platform over internet. Security features of SAI include local in-house servers and coding. The application has been vetted by CERT-in empanelled auditor and the Army Cyber Group.[24]

On October 1, Airtel announced the launch of its security intelligence centre (SOC) in the national capital region. The SOC will use Artificial Intelligence (AI) and Machine Learning (ML) tools to mitigate potential security risks, stemming from phishing attacks and denial of services, in partnership with several vendors. The company has also launched "Airtel Secure", a suite of cybersecurity solutions for enterprise customers.[25]

[23] https://dst.gov.in/mous-premier-academic-institutions-boost-manufacture-establishment-supercomputing-infrastructure

[24] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1668346

[25] https://www.lightreading.com/indias-airtel-puts-$13m-in-security-intelligence-center/d/d-id/764384

International Developments

Activities in global Cyber Space

Widespread Cyber-attacks as part of the hybrid warfare between Armenia and Azerbaijan has been revealed by Cisco's threat intelligence unit, on October 9, 2020.[26] Reportedly an Armenian Group hacked Azerbaijan's naval base and downloaded documents, including data associated with the commanders of warships, sailors, engineers and others associated with the Azerbaijani naval battalion.[27]

In another development the U.S. Department of Justice on October 19, charged six members of Russia's GRU (military intelligence agency), for their alleged role in several major cyberattacks over the past few years, that included the 2016 cyber-attacks on Ukraine's power grids and the 2017 French presidential election.[28]

On October 23, the U.S. Treasury Department imposed sanctions on a Russian research centre, the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM), for having connections with the "Triton malware". The malware made headlines in 2017 after it was deployed at a petrochemical plant in Saudi Arabia, sabotaging safety systems and risking an explosion. Triton's creators have also been accused of probing attacks on upwards of twenty U.S. electric utilities in 2019.[29]

The European Union on October 22, imposed sanctions on two Russian officials and a part of Russia's GRU (military intelligence agency) over a cyberattack against the German parliament in 2015. This attack targeted the parliament's information system and affected its operations for several days. The same GRU unit earlier was accused of trying to hack into the Wi-Fi network of the Organization for the Prohibition of Chemical Weapons, based in the Netherlands, in 2018.[30]

[26] https://blog.talosintelligence.com/2020/10/poetrat-update.html

[27] https://internetgov.news/internet-gov-weekly-brief-w41a20-un-desa-publish-compendium-of-digital-gov-initiatives-us-congress-releases-tech-antitrust-report-uneca-launch-africa-data-initiative-ecj-ruling/

[28] https://www.securityweek.com/us-charges-russian-intelligence-officers-notpetya-industroyer-attacks

[29] https://ciso.economictimes.indiatimes.com/news/us-sanctions-russian-govt-institution-tied-to-malware/78843023

[30] https://www.securityweek.com/eu-slaps-sanctions-2-russians-over-germany-cyberattack

Digital Technologies

Semiconductor Technology

Semiconductor industry in the US is consolidating with landmark transactions, boosted by cloud computing and requirements of personal computers during COVID-19. Advanced Micro Devices Inc. (AMD) announced on October 27, 2020 plans to buy rival chip maker Xilinx Inc. in a $35 billion deal. AMD specializes in central-processing units and graphics chips for computers. Xilinx would give AMD a foothold in areas where it is a small player or entirely absent, including telecommunications infrastructure and defence. Xilinx chips are used in the U.S.'s latest combat plane, the F-35 Joint Strike Fighter as also in the superfast 5G network infrastructure.[31]

Earlier, Graphics chip maker Nvidia acquired ARM Holdings for about $40 billion. In July, Analog Devices bought Maxim Integrated Products for $20 billion. Both Nvidia and AMD outsource chip manufacturing to the Taiwan Semiconductor Manufacturing Corporation (TSMC).[32]

5G Technology

Washington has stepped up its offensive against Huawei, offering financing to get the Chinese telco effectively blocked from Brazil's next-generation 5G networks. Towards this Export-Import Bank of the United States (EXIM) signed a memorandum of understanding with Brazil to "identify potential opportunities" in the fields of energy, telecommunications and 5G for financing up to $1 billion. US maintains that Huawei represents a national security threat, a claim denied by Huawei.[33]

Artificial Intelligence

On October 21, 2020, Saudi Arabia launched a multibillion-dollar strategy, to become a global leader in artificial intelligence (AI) and data by 2030. It aims to train 20,000 specialists and experts, have 300 active start-ups and attract $20 billion in national and foreign investments in the field of data and AI.[34]

[31] https://www.wsj.com/articles/amd-agrees-to-buy-rival-chip-maker-xilinx-for-35-billion-11603794663

[32] ET Prime October 29, 2020

[33] https://www.cnbc.com/2020/10/21/us-tries-to-get-huawei-blocked-from-brazils-5g-networks.html

[34] https://www.arabnews.com/node/1752096/saudi-arabia

South Korea too is targeting to develop up to 50 types of artificial intelligence-focused system semiconductors by 2030. South Korea is the leader in Dynamic Random-Access Memory (DRAM) chip market. The AI chip market is expected to grow rapidly, according to the Korea Information Society Development Institute.[35]

It is likely to reach USD117.9 billion by 2030, as compared to USD18.5 billion today.

Strategy/Policy

The U.S. National Security Council, on October 13, issued the "National Strategy for Critical and Emerging Technologies (C&ET)". C&ET are defined as those technologies that have been identified and assessed by the National Security Council (NSC) to be critical, or potentially critical, to the United States' national security, including military, intelligence, and economic advantages. These include artificial intelligence, quantum information science, and semiconductors. The objective of the strategy is to ensure that the United States, with its allies and partners, continue to be the world leader in C&ET by implementing two necessary pillars of success: 'promoting the National Security Innovation Base' (NSIB), and 'protecting technology advantage'. The strategy calls for a strong export control system that regulates which technologies can be sent abroad.[36]

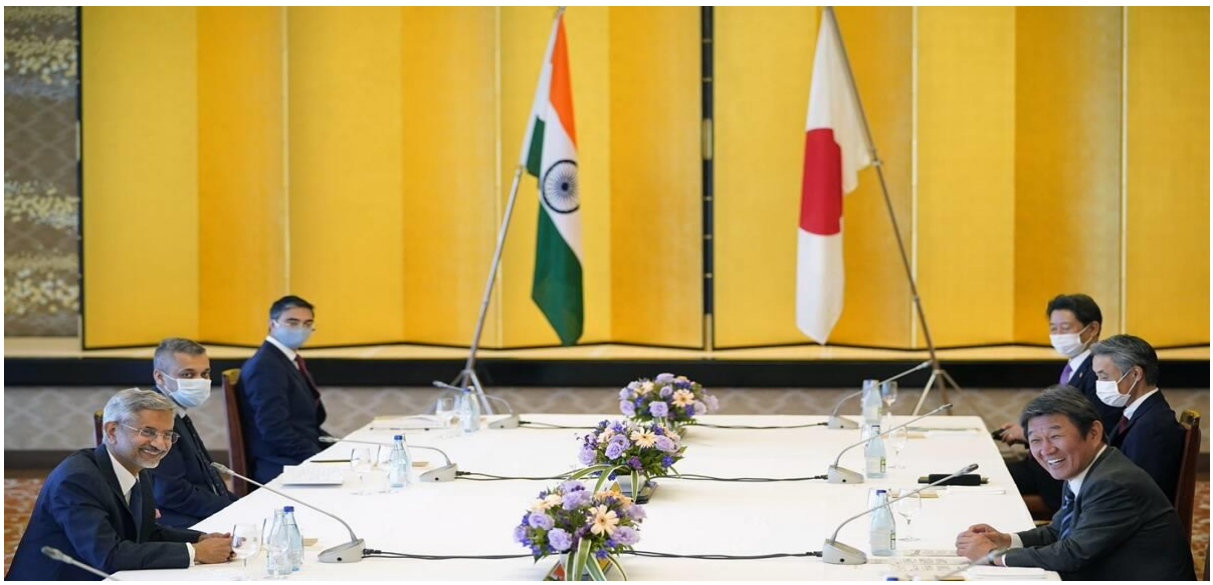
[35] https://www.expresscomputer.in/artificial-intelligence-ai/s-korea-aims-to-develop-50-ai-chips-by-2030/64912/

[36] https://www.whitehouse.gov/wp-content/uploads/2020/10/National-Strategy-for-CET.pdf

International Cooperation

Bilateral/Minilateral Cooperation

The Union Cabinet, on October 7 and October 29, approved the signing a Memorandum of Cooperation (MoC) in the field of cybersecurity and Information and Communication Technologies (ICTs) between India and Japan.[37] The MoC, will enhance cooperation in these fields by developing joint mechanisms for practical cooperation to mitigate cyber threats to the security of Information Communication Technology (ICT) infrastructure as also contribute in strengthening bilateral cooperation and mutual understanding in the field of communications and emerging technologies like 5G network, telecom security, Artificial Intelligence (AI), Block Chain etc.



Foreign Minister Subrahmanyam Jaishankar, left, and his Japanese counterpart Toshimitsu Motegi, right, smile at the start of their luncheon meeting at the Iikura Guest House in Tokyo, Japan. (AP)(https://indianexpress.com/article/india/india-japan-close-to-cybersecurity-deal-call-for-robust-digital-ecosystem-6709898/)

According to a Statement on end-to-end encryption and public safety released by the US Justice Department on October 11, members of the intelligence-sharing "The Five Eyes" alliance, comprised of the US, the UK, Canada, Australia, and New Zealand, along with Japan and India, have noted that law enforcement has a responsibility to protect citizens of the country and urged industry to address concerns of end to end encryption, which precludes any legal access to content, by Law Enforcement Authorities (LEA). They called on technology companies to enable lawful access to content in a readable and

[37] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1662334

usable format and formulate design decisions, including backdoors.[38] Digital rights advocacy groups including the Internet Freedom Foundation (IFF) have objected to this move of calling on technology companies to allow backdoor access to encrypted communication.[39]

Multilateral Cooperation

On October 26, the Chair of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security ("OEWG") addressed a letter to all Permanent Representatives and Permanent Observers to the United Nations, giving out the draft program of the next virtual meetings of OEWG from 17 to 19 November, 2020. The meeting will focus on the themes of confidence-building and capacity-building measures in cyber space.[40]

[38] https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

[39] https://telecom.economictimes.indiatimes.com/news/digital-rights-body-questions-indias-move-to-seek-backdoor-access-to-encrypted-communication/78659433

[40] https://front.un-arm.org/wp-content/uploads/2020/10/201026-oewg-chair-letter-on-the-third-round-of-informal-meetings.pdf

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

www.delhipolicygroup.org