Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

NOVEMBER 2020

Volume I, Issue 10 | November 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 10
November 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 10
November 2020

Contents

Abstract

In recent months, there has been an increase in ransomware attacks on Indian industries, mainly pharmaceutical companies. These attacks have mostly emanated from China and Pakistan, mirroring prevailing geopolitical tensions. A recent survey has predicted that nation-state attacks will be the biggest concern for 2021. To combat these challenges, the Indian establishment is working out strategies, including banning mobile apps that are engaged in activities prejudicial to national security.

Technological capabilities being the key to secure cyber space, the Prime Minister has exhorted young talent in the country to create robust cyber security solutions to protect data. National technological capabilities have received a boost with the launch of Indian radar imaging satellite EOS-01, equipped with synthetic aperture radar that can take pictures in all weather conditions.

The indigenously developed Indian Regional Navigation Satellite System (IRNSS) received global recognition by being recognised as a component of the World-Wide Radio Navigation System from the International Maritime Organisation. In addition, India's radio interface technology (5Gi) has been evaluated by ITU and deemed to be conforming to the global 5G standard. Further, the Indian supercomputer 'Param Siddhi' achieved the global ranking of 63 among the top 500 most powerful non-distributed computer systems in the world.

Recognising the criticality of building an indigenous and secured telecom infrastructure, the government has included telecom & networking products as part of the Production-Linked Incentive (PLI) scheme which is designed to provide budgetary support to 10 key sectors. This is in addition to the already notified PLI scheme in mobile manufacturing.

Global cyber space continues to be affected by ransom-driven 'denial of service' attacks by several hacker groups like Fancy Bear, Cozy Bear and Lazarus. These groups are suspected to be associated with particular nation states. Global and bilateral collaboration along with regulatory norms are considered essential to deal with this menace. The US National Security Commission on Artificial Intelligence has proposed a formal alliance with India and other nations in the Indo-Pacific region to develop an overarching Indo-Pacific security strategy focused on emerging technologies.

On the regulatory side, European Union lawmakers have proposed a new set of rules for exporting dual use products and technologies, including cyber-surveillance tools. Similarly, a new telecommunications (security) Bill has been introduced in the British Parliament proposing to block high-risk equipment suppliers and tighten security requirements for new high-speed fibre optic and 5G wireless networks.

At the virtual 15th G20 summit on November 21, the Prime Minister proposed a global index for the post-Corona world, based on talent, technology, transparency and trusteeship. He also suggested the creation of a G20 Virtual Secretariat as a follow up and documentation repository. Similar views were also echoed by India at the 15th annual Meeting of the Internet Governance Forum (IGF) organised by the United Nations, which recognised the world's increased reliance on the internet during the Covid-19 pandemic and called for digital inclusion to build a strong recovery.

National Developments

Cyber Threat Scenario

Cyber-attacks on Indian industries have increased in recent times. During the month, pharmaceutical companies, including Dr. Reddy's and Lupin, reported ransomware attacks. Grocery platform Big Basket's data was compromised and personal information of some 20 million users was put on sale on the dark web. A probe on the power outage in Mumbai last month revealed that there were multiple suspicious log-ins to the servers of the power supply and transmission utilities by accounts operating from South Asian countries.[1] During the month, Microsoft detected cyber-attacks targeting prominent companies involved in vaccine research and treatment for Covid-19, including in India.[2]

According to the 2020 Global Cyber Security Attitude Survey released on November 18, Indian organisations were the worst hit by ransomware attacks among all Asia Pacific (APAC) nations during the Covid-19 pandemic and globally India Inc. stood second. More than one-third (34%) of Indian organisations paid between $1 million – $ 2.5 million to hackers to get back their data and system access during the last 12 months. India Inc. is particularly threatened by cyber-attacks originating from China and Pakistan, due to prevailing geopolitical tensions. The Survey added that nation-state attacks will be the biggest concern for 2021.[3]

However, legal enforcement to fine or prosecute these companies for lax security of data or to legally attribute these attacks has been a challenge.[4] Indian National Cyber Security Coordinator (NCSC) and security agencies are working out strategies to deal with the menace and take legal and regulatory measures to plug the gaps. The Indian Computer Emergency Response Team (CERT-In), which issues advisories regarding vulnerabilities, issued an alert on November 4 regarding ransomware virus "Egregor" that

[1] https://www.financialexpress.com/opinion/get-cybersecurity-right-mumbai-power-failure-shows-firefighting-cant-be-a-response/2136767/

[2] https://www.financialexpress.com/industry/technology/russian-north-korean-hackers-targeting-vaccine-work-alleges-microsoft-alleges/2128271/

[3] https://ciso.economictimes.indiatimes.com/news/india-is-second-in-global-ransom-payouts-for-cyberattacks-survey/79295374

[4] https://cio.economictimes.indiatimes.com/news/digital-security/who-stole-my-data/79361807

threatens to release sensitive corporate data of the victim organisation if not compensated.[5]

Referring to China as a major "challenge", the National Cyber Security Coordinator, Lt. Gen. (Dr) Rajesh Pant, highlighted that each day 4 lakh malwares are discovered and 375 cyber-attacks are witnessed from China. He indicated that the forthcoming National Cyber Security Strategy is expected to have 40 deliverables to address various challenges in cyber space. These include common but differentiated responsibilities, cyber hygiene, critical information infrastructure protection, cyber audit, malware repository and a programme for responsible vulnerability disclosure. He also emphasised the need for indigenisation of both cyber security products and services to prevent data loss.

To protect sensitive data of Indian citizens, on November 24 the Indian government blocked 43 Chinese mobile applications for engaging in activities seen as prejudicial to national sovereignty and integrity.[6] With this order, the total number of Chinese-origin apps banned by India has gone up to 267. The Chinese embassy in India, while protesting the ban, contended that the move violated the rules of the World Trade Organization (WTO).[7]

Digital Technologies

Technology is the key to a secured cyber space. Virtually addressing the Bengaluru Tech Summit 2020 (BTS2020) on November 19, the Prime Minister exhorted young talent to create robust cyber security solutions to protect data and IT infrastructure with the potential to go global, while laying emphasis on a sound data governance framework.[8] The Prime Minister further highlighted that technology is redefining the defence sector with indigenous software and emerging technologies.[9]

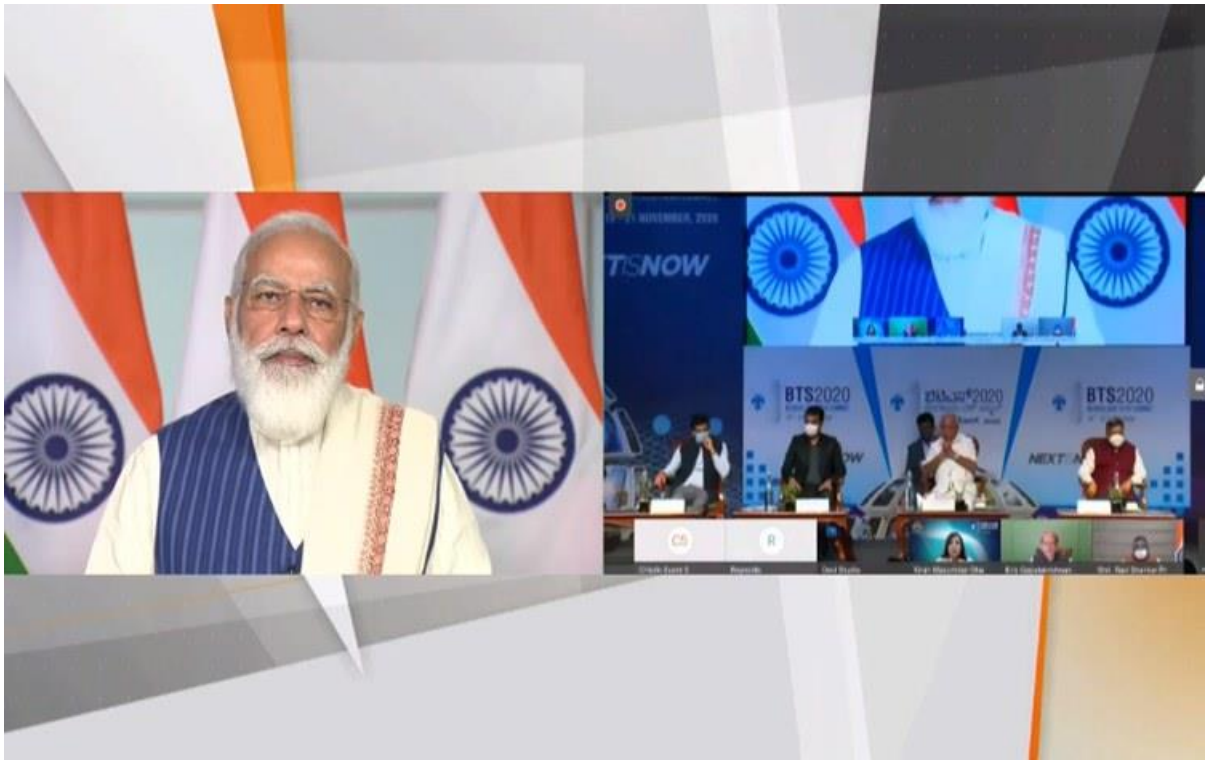
[5] https://www.outlookindia.com/newsscroll/cyber-agency-alerts-against-ransomware-attacks-of-egregor-virus/1969840

[6] https://telecom.economictimes.indiatimes.com/news/india-bans-43-new-chinese-apps-including-snack-video-aliexpress/79389424

[7] https://www.hindustantimes.com/india-news/china-says-india-s-latest-app-ban-order-violates-wto-rules/story-xgktTlRi1Jyg06C3rmC6xJ.html

[8] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1673951

[9] http://www.newsonair.com/News?title=PM-Modi-to-inaugurate-Bengaluru-Tech-Summit-2020-today&id=404511



Prime Minister Narendra Modi virtually inaugurating the Bangalore Technology Summit on November 19, 2020 (http://www.newsonair.com)

Echoing this vision at the Global R&D Summit 2020 organised by FICCI, Amitabh Kant, CEO of NITI Aayog, highlighted that India can create up to $1 trillion worth of economic value through the digital economy by 2025, providing an attractive opportunity for global and local businesses, start-ups and innovators to invest in emerging technologies like Artificial Intelligence, Blockchain and drones, customised to Indian needs.[10]

Space Technology

Giving a boost to India's space-based surveillance, a radar imaging earth observation satellite (EOS-01) was launched on November 07 by India's Polar Satellite Launch Vehicle (PSLV-C49) from the Satish Dhawan Space Centre in Sriharikota. EOS-01 is equipped with synthetic aperture radar (SAR) that can take pictures in all types of weather conditions, boosting both military and civil surveillance capability.[11]

[10] http://www.ficci.in/pressrelease-page.asp?nid=3990

[11] https://swarajyamag.com/insta/isros-pslv-c49-successfully-inserts-indian-earth-observation-satellite-eos-01-nine-foreign-satellites-into-orbit

PSLV-C49 Lifts-off (https://www.isro.gov.in/)

The International Maritime Organisation (IMO) at its meeting in November, 2020 accorded the Indian Regional Navigation Satellite System (IRNSS) the coveted recognition as a component of the World-Wide Radio Navigation System.[12] IRNSS will provide accurate positional information services to assist the navigation of ships in the Indian Ocean up to 1500 km from the Indian coastline.[13]

5G Technology

Virtualisation of the 5G network, by adopting open radio access network (O-RAN) technology, will help disaggregate hardware and software modules, reduce cost of deployment of 5G and enhance interoperability. O-RAN architecture uses programmable software solutions with open interfaces. All Indian telecom operators are presently conducting trials on this technology. On November 12 Airtel indicated that as a member of the O-RAN alliance, it is currently working with various US and Japanese vendors like Altiostar and NEC to develop O-RAN based innovative solutions for 5G telecom equipment.[14] Similarly, Vodafone Idea has been engaged with partners like Mavenir within the O-RAN space to develop solutions suitable to the traffic requirements of Indian networks.

Meanwhile, India's own radio interface technology, developed by the Telecom Standards Development Society of India (5Gi), has successfully completed the

[12] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1674483

[13] https://eurasiantimes.com/the-indian-navigation-satellite-system-irnss-approved-by-imp-for-global-operations/

[14] https://telecom.economictimes.indiatimes.com/news/bharti-airtel-hosts-indias-first-o-ran-alliance-plugfest/79187934

evaluation phase of the ITU's International Mobile Telecommunications 2020 (IMT-2020) vision and requirements for the globalisation of 5G. According to a ITU press release of November 26, this technology is deemed to be sufficiently detailed to enable worldwide compatibility of operation and conforms to the global 5G standard.[15]

Artificial Intelligence

Recognising the importance of AI, the Indian Government has focussed on building super computers. The Indian high-performance computing-artificial intelligence (HPC-AI) supercomputer named 'Param Siddhi', built under the National Supercomputing Mission (NSM), has achieved the global ranking of 63 among the top 500 most powerful non-distributed computer systems in the world, it was notified by the Ministry of Science and Technology on November 18, 2020. With the infusion of Param Siddhi-AI, the scientific and technological community in the country has been empowered to solve multidisciplinary challenges, including in healthcare, agriculture, education, energy, cybersecurity, urban planning, space, AI applications and climate modelling.[16]

The S&T ministry had earlier announced that the third phase of the NSM will commence in January 2021, taking computing speed to around 45 petaflops. Japan's 'Fugaku', jointly developed by RIKEN and Fujitsu, is currently the fastest supercomputer in the world, with a speed of 415 petaflops.

Blockchain Technology

Several countries including China are experimenting with digital currencies. A Central Bank Digital Currency (CBDC) is a digital payment instrument that is denominated in a national currency and issued by a central bank. Developing economies look at CBDCs as a financial inclusion tool, while developed economies look at it for either improving their payment systems or for geo-political reasons.[17]

Earlier this year, the National Institute for Smart Government (NISG) had proposed the concept of a Central Bank Digital INR (CBDR) administered through a national permissioned blockchain, in its draft National Strategy on Blockchain. The aim of this strategy is that India will be one of the leading countries in the world in innovation, education, commercialisation and

[15] https://www.itu.int/en/mediacentre/Pages/pr26-2020-evaluation-global-affirmation-imt-2020-5g.aspx

[16] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1673715

[17] https://www.bloombergquint.com/business/central-banks-are-hastening-the-move-towards-digital-currencies

adoption of blockchain technology in private and public sectors by 2025. The CBDR could address the disconnect between India's 1.2 billion mobile connections and only 582 million bank accounts, a void often filled by cryptocurrencies like Bitcoin, which the government is striving to address.[18]

[18] https://www.businesstelegraph.co.uk/indian-central-bank-digital-currency-proposed-finextra/

National Initiatives

Strategy/Policy

The Ministry of Electronics & Information Technology released a draft data Centre policy-2020, which works towards providing "infrastructure status" for the data centre sector, at par with other sectors like railways, roadways, and power.[19] Data Centres are also proposed to be declared as an essential service under the "The Essential Services Maintenance Act, 1968 (ESMA)". Also, recognising the need for uninterrupted power supply, the policy would facilitate captive power generation and use of renewable energy.[20]

Budgetary Support

Telecom equipment forms a critical and strategic element of building a secured telecom infrastructure. India aspires to become a major original equipment manufacturer of telecom and networking products. To meet this objective, on November 11 the Union Cabinet approved a Production-Linked Incentive (PLI) Scheme in 10 key sectors for enhancing India's manufacturing capabilities and exports. These are in addition to the already notified PLI schemes in mobile manufacturing and specified electronic components, and include electronics/technology products and telecom & networking products.[21]

Capability Building

To build capabilities in cybersecurity research and development, multi-stakeholder collaboration between governments, industry, research institutions and innovative start-ups are needed. With this aim, on November 9 the National Centre of excellence for cyber security technology development and product entrepreneurship hosted a virtual roadshow on India's cybersecurity R&D capabilities. The exhibition brought together key government stakeholders, leading academic institutions, user organisations, multinational firms and venture capitalists on one platform and showcased 20 leading research projects in the area of cybersecurity and emerging technologies.

In a special address at the event, Lt. Gen. (Dr.) Rajesh Pant, National Cyber Security Coordinator, lamented that India as a nation is spending 1 per cent of GDP for cybersecurity R&D, out of which the private sector is spending only 0.3

[19] Draft Data Centre Policy - 03112020_v5.5.pdf

[20] https://telecom.economictimes.indiatimes.com/news/meitys-draft-data-centre-policy-assigns-infrastructure-status-to-the-sector/79095109

[21] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1671912

per cent. The largest R&D centres of global companies are in India, yet the research spending towards Indian capabilities remains low. He urged Indian industry to spend more on cyber security R&D.[22]

[22] http://www.businessworld.in/article/Virtual-roadshow-on-India-s-cybersecurity-R-amp-D-capabilities-to-provide-platform-to-academia-research-institutes-PSUs/09-11-2020-340855/#

International Developments

Activities in Global Cyber Space

Supply chain vulnerability has been a global security concern. A case in point is that of the infamous Lazarus Group, targeting South Korean supply chains, as per a warning by cybersecurity researchers of ESET in their November 16, 2020 report. The attackers abused legitimate South Korean security software and digital certificates stolen from different companies to deploy their malware. These hackers are particularly interested in supply chain attacks, because they allow them to covertly deploy malware on many computers at the same time.[23] The Lazarus Group was blamed for the 2014 cyber-attack on Sony Pictures Entertainment and the 2017 WannaCry ransomware attack on various countries, including the US and Britain.

Another global menace has been 'denial of service' attacks on critical infrastructure. On November 23, CircleID, a leading global platform for Internet developments, warned of a significant increase of distributed denial of service (DDoS) attacks and their level of sophistication. In 2020, these numbers showed a four-fold increase compared to the pre-COVID-19 level. While most attacks are under 500 Mbps and 1 Mbps, they are still capable of causing service disruptions. Ransom-driven DDoS attacks are on the rise, as hacker groups like Fancy Bear, Cozy Bear and the Lazarus Group extort organisations around the world.[24]

It is interesting to note that cyber-attacks on the US election system continue even after the conclusion of voting. On November 18, a subdomain of the official Joe Biden campaign website 'vote.joebiden.com', sponsored by the Democratic National Committee (DNC), was defaced, apparently by a Turkish hacktivist called "RootAyyıldız," describing himself as a "Turkish and Muslim defacer" and a patriot. The message threatened Turkey's adversaries and Turkish political parties backed by the United States.[25]

[23] https://ciso.economictimes.indiatimes.com/news/hacking-group-lazarus-targets-south-korean-supply-chains/79255273

[24] CircleID Weekly Wrap for 2020-11-24

[25] https://www.securityweek.com/subdomain-official-joe-biden-campaign-website-defaced-turkish-hacker

Digital Technologies

Semiconductor Technology

Semiconductor technology is at the centre of the US-China technology cold war. In September this year, American semiconductor companies were asked to stop selling advanced semiconductors and other technology to Chinese technology firms implicated in national security or human rights issues. However, on November 13, the U.S. government granted an exemption to Qualcomm Inc. to sell 4G mobile phone chips to China's Huawei Technologies Co Ltd. Huawei's potential to design its own chips has been thwarted by U.S. trade restrictions that blocked its access to chip design software and fabrication tools.[26]

While this exemption was granted, the US media reported on November 22 that semiconductor chips made by American semiconductor companies like Intel and Nvidia power a supercomputing centre used by the Chinese government to track people in Xinjiang, for surveillance and suppression of minorities.[27]

5G Technology

The allocation of 5G frequency spectrum has remained a global challenge. The French national telecoms regulatory authority, 'Arcep', recently concluded a frequency auction that will enable 5G phone networks to go live in France soon. The regulator said that the auction brought in 2.8 billion euros ($ 3.3 billion) from four of its network operators. It added that their 5G networks could begin commercial operations after completing administrative formalities by last week of November 2020.[28]

Internet of Things

The fast-expanding field of "internet of things" (IoT) is set to become more widespread once 5G is deployed, posing serious threats to digital security in the future. As reported by Nokia, there has been a 100 percent increase in malware infections on IoT devices since last year. With each new application of 5G, criminals get opportunities for inflicting damage and extracting ransom.

[26] https://telecom.economictimes.indiatimes.com/news/qualcomm-receives-u-s-permission-to-sell-4g-chips-to-huawei-in-exception-to-ban/79218859

[27] https://www.nytimes.com/2020/11/22/technology/china-intel-nvidia-xinjiang.html

[28] https://www.france24.com/en/20201001-french-government-rakes-in-%E2%82%AC2-8bn-from-5g-frequency-auctions-to-mobile-operators

At a conference hosted on November 17, "friendly hacker" Keren Elazari said that the earlier trend of the Silicon Valley employing ethical hackers to hunt for vulnerabilities as part of a bug-bounty programme is now being practiced by organisations ranging from the Pentagon to banks and airlines, tech giants and smaller businesses. The largest bug-bounty platform, 'Hacker One', has 800,000 hackers on its books and the organisation has paid out a record $44 million (38.2 million euros) in cash rewards this year, up 87 percent on the previous 12 months.[29]

Artificial Intelligence

Collaboration among friendly nations is essential to develop digital technologies. Recognising this, the US National Security Commission on Artificial Intelligence, in a recent report, recommended that the Department of State and the Department of Defence should formalise a technology alliance with India, Australia, Japan, New Zealand, South Korea, Vietnam and other nations in the Indo-Pacific region to focus on AI cooperation for defence and security purposes.[30]

It is predicted by strategic experts that artificial intelligence and quantum information science would remain key priorities for the new US administration and overall spending on research and development is expected to be higher. The Biden campaign had proposed an innovation funding of $300 billion over four years, in addition to federal research and development spending, to remain competitive with China in technologies such as AI, quantum computing, clean energy and 5G, according to the campaign's website.[31]

Strategy/Policy

Legal and regulatory measures are being considered globally to deter abuses in cyber space. A new set of rules for exporting dual use products and technologies, including cyber-surveillance tools, were finalised on November 9 by European Union lawmakers and the European Council, to prevent these from being used to violate human rights. These include facial recognition, high-performance computers, drones and certain chemicals. The current update, made necessary by technological developments and growing security risks, includes new criteria to grant or reject export licenses for certain items.

[29] https://www.securityweek.com/boom-demand-friendly-hackers-5g-approaches

[30] https://telecom.economictimes.indiatimes.com/news/us-body-on-artificial-intelligence-calls-for-creating-india-us-strategic-tech-alliance/78662022

[31] https://www.insidequantumtechnology.com/news/wsj-quantum-ai-rd-funding-to-remain-key-priorities-under-biden/

The agreement needs formal approval from the European Parliament and other bodies.[32]

Similarly, on November 24, a Telecommunications (Security) Bill was introduced in the British Parliament, that proposes imposition of strict security rules on telecommunication companies in the United Kingdom. The bill aims to block high-risk equipment suppliers and tighten security requirements for new high-speed fibre optic and 5G wireless networks. Under the bill, public telecoms providers are obliged to report security compromises and share information with the UK telecoms regulator, the Office of Communications (Ofcom), in order for the security of their networks to be assessed. If approved by the UK Parliament, companies which fail to meet deadlines for higher security requirements could face fines up to 10% of turnover or more than £100,000 a day in the case of "continuing contravention".[33]

[32] https://www.securityweek.com/eu-agrees-tighter-rules-surveillance-tech-exports

[33] https://www.bbc.com/news/technology-55044182

International Cooperation

Bilateral/Minilateral Cooperation

India has been actively pursuing bilateral/minilateral cooperation in the field of cyber security and collaboration for development of digital technologies. On November 4, the Union Cabinet approved signing of a Memorandum of Understanding (MoU) between India and the United Kingdom for co-operation in Telecommunications and Information & Communications Technology (ICT). The MoU will contribute towards strengthening bilateral cooperation and mutual understanding between the two sides in the field of Communication Technologies, an official release said.[34] Areas for cooperation include technological development in telecom/ICT including 5G, internet of things, R&D on emerging technologies, spectrum management and security of telecommunication infrastructure.

Multilateral Cooperation

G20 leaders at the G20 Riyadh Summit held on November 21, 2020. Twitter/@g20org

Prime Minister Narendra Modi attended the virtual meeting of the 15th G20 Summit chaired by the Kingdom of Saudi Arabia on November 21. At the meeting, he stressed the need for a global index for the post-Coronavirus world based on talent, technology, transparency and trusteeship towards the planet. "Value of new technologies should be measured by their benefit to humanity," he added.[35] Noting that 'Work from Anywhere' is a new normal in the post

[34] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1670015

[35] https://www.indiatoday.in/india/story/pm-modi-at-g20-summit-speaks-on-covid-turning-point-1742931-2020-11-21

COVID-19 world, PM Modi also suggested the creation of a G20 Virtual Secretariat as a follow up and documentation repository.[36]

The Fifteenth Annual Meeting of the Internet Governance Forum (IGF) was hosted online by the United Nations from November 2-17 under the overarching theme "Internet for human resilience and solidarity". The event featured discussions on a range of issues including data, environment and trust. The IGF meet recognised the world's increased reliance on the Internet during the pandemic and focused on digital inclusion, which is essential to build a strong recovery.[37]

[36] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1674827

[37] https://www.intgovforum.org/multilingual/content/igf-2020-outputs

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

www.delhipolicygroup.org