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

DPG CYBER REVIEW

OCTOBER 2022

Volume III, Issue 10 | October 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 10
October 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 10
October 2022

Contents

Abstract

Pakistan has set up a clandestine Cyber-Army with help from Turkey, for working against perceived influence operations pursued by the US, India, and other foreign powers. Approximately 6,000 Pakistani police officers have been trained since 2018, to shape public opinion for domestic political goals and influence the views of Muslims in Southeast Asia.

Tata Power suffered a ransomware attack, on its IT infrastructure and some of its IT systems were impacted. The Central Bureau of Investigation (CBI) launched "Operation Chakra" at 115 locations, in coordination with Interpol, FBI, Royal Canadian Mounted Police, Australian Federal Police, with assistance from multiple state police, against international cyber-criminal gangs involved in financial crimes.

5G rollout in India has been delayed for want of over-the-air (OTA) software update on mobiles to connect to high speed 5G network. The Government and stake holders including telecom operators and handset makers are interacting to resolve teething issues for expediting the roll-out. Network equipment makers are also interacting with telecom operators to deploy 5G Radio Access Network (RAN) products and solutions. Competitions have intensified among satcom operators to enter India's broadband-from-space services segment, which could be worth $13 billion by 2025. 36 broadband communication satellites of OneWeb were launched into orbit by ISRO, as part of its maiden commercial mission. One Web's broadband-from-space services in India is likely to start in 2023. SpaceX has applied for the required licence for its Starlink network.

The Indian government intends to spend up to $ 1.3 billion to modernise and upgrade the Semi-conductor Laboratory (SCL) in Mohali, Punjab, that produces chips for strategic purposes.

The Government has notified further reforms in tele-communications (Wireless Licencing), satellite communication and has updated National Frequency Allocation Plan, to facilitate ease of doing business, and attracting investments.

On the international front, a hacktivists group "Black Reward", supporting mass protests in Iran, following the death of Mahasa Amin in September, have stolen information from Iran's Atomic Energy Organisation. The group has demanded the release of prisoners detained during the ongoing protests in exchange for the data.

European Union countries, including Slovakia, Poland and Germany are increasingly encountering cyber-attacks, as they help Ukraine in the ongoing Russia-Ukraine War. Pro-Russian hackers also attacked airport websites of several major US cities that affected flight and services information. Several Chinese were suspended from the inhouse Chinese app "WeChat", after two banners protesting Chinese Rule were circulated online, just prior to the Chinese Communist Party Congress-2022.

The $44 Billion takeover of Twitter by Elon Musk is marked by swift changes with his characteristic imprint, that has caused a major upheaval in the international communities about the social media platform.

Tightening further regulations on China, the US administration announced a new export controls policy that restricts transactions involving technologies, expertise and materials for artificial intelligence, supercomputer, and semiconductor manufacturing, in its bid to slow Beijing's technological and military advances. US citizens including green card holders, are prohibited from supporting the development or production of advanced chips in China.

The US President released "The National Security Strategy-2022", that lists the security concerns and challenges of the US and the plans to deal with them. The main thrust of the strategy is to compete with China and contain Russia, by investing in technologies at home, building a coalition of like-minded states, and modernizing its military. It aims to deter cyber-attacks from state and non-state actors by responding with all appropriate tools of national power and professes to promote adherence to the UN endorsed framework of responsible state behaviour in cyberspace.

The 90th General Assembly Meeting of the International criminal police organisation (INTERPOL), with 195 member countries, was hosted by India in New Delhi. The meeting discussed the importance of technology like artificial intelligence and the metaverse for agile policing to deal with the changes taking place in the global cyber threats landscape.

National Developments

Pakistan set up cyber-army against India with help from Turkey

It was reported on October 27 that Pakistan has set up a clandestine Cyber-Army, camouflaged under a bilateral agreement with Turkey on cooperation against cybercrime, to work against perceived influence operations by the US, India, and other foreign powers. The cooperation has continued since 2018, with some 6,000 Pakistani police officers trained by Turkey for this and other projects.

The Cyber-Army is used to shape public opinion, influence the views of Muslims in Southeast Asia, attack the US and India, and undermine criticism levelled against the Pakistani rulers.[1] The modus operandi includes hacking opponents' emails and social media accounts, collecting private data from cell phones and computers, and using the hacked material to intimidate and at times blackmail victims.[2]

On October 13, the Interior Minister of Turkey-Soylu made an indirect reference to this clandestine operation during an interview with a local TV Channel. Soylu himself is infamous for running troll and bot armies in cyberspace to undermine public view of the opposition and dissenters and had worked on similar covert operations even before he became a minister in September 2016.[3]

Tata Power's IT Systems affected due to cyberattack

It was reported on October 14, that Tata Power had suffered a cyberattack on its IT infrastructure and some of its IT systems were impacted. Tata Power is in the process of retrieving and restoring their systems. The company maintains that its critical operations were not affected, although as a precautionary measure "restricted access and preventive checks" have been put in place at all employee and customer-facing portals and touch points.[4]

[1] https://theprint.in/world/turkey-assisted-pakistan-in-setting-up-secret-cyber-army-against-us-india/1183559/

[2] Pakistan set up cyber army against India with Turkey's help: Report | World News - Hindustan Times

[3] https://nordicmonitor.com/2022/10/turkey-helped-pakistan-set-up-a-secret-cyber-army-for-influence-operation-against-us-india/

[4] Tata Power cyberattack impacted IT systems; bill payment portal down for a week, IT Security News, ET CISO (indiatimes.com)

On October 26, several important data, including bank accounts of the company, bank statements as well as details of Tata Power employees were leaked on the dark web, by a ransomware gang "Hive", which is a ransomware-as-a service (RaaS) operator that provides a subscription model for cybercriminals to become affiliates. It's likely the data was leaked due to failed ransom negotiations. "Hive" targets sectors like energy, healthcare, financial services, media, and education together with other ransomware affiliates, solely driven by financial gains.[5]

CBI crackdown on cyber criminals at 115 locations

On October 8, the CBI launched "Operation Chakra" in coordination with Interpol, FBI, Royal Canadian Mounted Police and Australian Federal Police, with assistance from several State police, against international cyber-criminal gangs involved in financial crimes. The operation was carried out at 115 locations, with the intention to dismantle the infrastructure of these international cybercrime gangs in India and bring these perpetrators to justice. Huge digital evidence including mobiles, laptops, etc. have also been recovered. Two call centres in Pune and Ahmedabad have been busted.[6]

Efforts to streamline issues for early 5G rollout

Despite the announcement of the roll out of 5G on October 1, Operationalisation of 5G network has been delayed as majority of mobile sets need an over-the-air (OTA) software update to connect to 5G network. It was reported on October 11, that the Government has called for a meeting of all stake holders in the government and industry including handset makers, to work on resolving issues and expediting the roll-out. The agenda includes holding talks "to prioritise" and release software upgrades for supporting the high-speed network.

Reportedly, Apple is extensively testing its 5G iPhone models on both Airtel and Reliance Jio's 5G network and may roll out the updates by December 2022. Network equipment makers like Nokia, Ericsson and CISCO are also interacting with telecom operators to deploy 5G Radio Access Network (RAN) products and solutions, and E-band microwave mobile transport solutions. Both Airtel and

[5] Hive: Tata Power data leak: What makes Hive "one of the top 5 ransomware groups operating today", IT Security News, ET CISO (indiatimes.com)

[6] CBI crackdown on cyber criminals; Search ops at 115 locations, IT Security News, ET CISO (indiatimes.com)

Reliance Jio aim to cover the entire country with fifth-generation networks between 2023-2024.[7]

Internet penetration is another issue of concern for early roll out of 5G. Nearly 75% of rural India does not have access to broadband as many locations are still without cellular or fibre connectivity. On October 27, telecom operators have been urged by the Union IT Minister to add on at least 10,000 base trans-receiver stations (BTS) every week compared with the 2,500 BTSs that are being added per week now, to speed up the spread of 5G services in the country.[8]

Broadband from Space to augment reach of 5G

While the rollout of terrestrial 5G networks has been a priority, satellite communications operators have intensified their efforts to enter India's broadband-from-space services segment, which could be worth $13 billion by 2025. It was reported on October 18, that Jio Satellites (JSCL), Bharti-OneWeb, and Elon Musk-owned SpaceX have applied to the Department of Telecommunications (DoT) for a global mobile personal communication by satellite services (GMPCS) licence to launch broadband-from space services in India. DOT is awaiting the recommendations of Telecom Regulatory Authority of India (TRAI) over the new space communications policy, including the mode of spectrum allocation for satellite communications.

Some of the Satellite operators have contended that spectrum for space internet services should be given administratively and not auctioned on the lines of 5G services, as these airwaves are shared, required in remote areas, including desert, the Himalayas or oil rigs, and may not be commercially gainful.[9]

Keeping up the tempo to usher in broadband-from-space communication, the Indian Space Research Organisation (ISRO) placed 36 broadband communication satellites of OneWeb into orbit on October 23, by its Launch Vehicle LVM3-M2, which took off from the Satish Dhawan Space Centre, in Sriharikota. This was ISRO's maiden commercial mission and One Web's 14th launch, bringing the constellation to 462 satellites. It is planning a fleet of 648 low-earth-orbit satellites that will deliver high-speed, low latency connectivity

[7] Reliance Jio: Ericsson bags long-term 5G SA deployment deal from Jio, Telecom News, ET Telecom (indiatimes.com)

[8] DoT: Centre releases procedural reforms, streamlines frequency allocation, Telecom News, ET Telecom (indiatimes.com)

[9] Starlink: SpaceX applies for DoT licence for broadband-from-space service, Telecom News, ET Telecom (indiatimes.com)

worldwide. One Web's broadband-from-space services in India will likely start from the middle of 2023.[10]

Procedural reforms announced for all modes of communications

On October 26, the DOT released telecom Reforms 2022 (Wireless Licencing), reforms in the satellite communication (satcom) and National Frequency Allocation Plan-2022 (NFAP), to facilitate ease of doing business, and attracting investments. In September 2021 the government had unveiled first set of telecom sector reforms, which allowed deferred payment of statutory dues and redefined adjusted gross revenue (AGR) among other major measures.

The Wireless Licensing Reforms - 2022 has simplified the Standing Advisory Committee on Frequency Allocation (SACFA) clearance guidelines (procedure for clearance of low power BTS/small cells on street furniture/infrastructure). Simplified import licensing through an online process and a self-declaration-based clearance has been adopted, to speed up deployment of crucial telecom equipment in the country.[11]

The reforms for satcom services aim to streamline various procedures and clearances apart from easing norms for obtaining the Global Mobile Personal Communication by Satellite (GMPCS) licence. It has set a goal to connect 1.2 billion Indians to the internet by 2025-26 where the role of satellite communications and space segment will be critical.[12]

NFAP is a master document for spectrum allocation and planning for industry and policy making. Under the new NFAP-2022, nearly 17GHz of new additional spectrum has been released for implementing 5G in all three segments of radio spectrum – below 1 GHz, between 1-6 GHz and above 6 GHz. The NFAP-2022 also delicensed 865-868 MHz spectrum band for Internet of Things (IoT) and Machine to Machine (M2M) communications.[13]

Plans to modernise government owned Semiconductor Fab Unit

The Indian government intends to spend up to $ 1.3 billion to modernise and upgrade the Semi-conductor Laboratory (SCL) in Mohali, Punjab, that produces

[10] ISRO completes LVM3-M2 commercial mission, places 36 OneWeb satellites (yourstory.com)

[11] Telecom Reforms: Wireless licensing reforms will enable ease of doing business, facilitate faster network roll outs: COAI, Telecom News, ET Telecom (indiatimes.com)

[12] Satellite Communication: Space technologies offer convergence, can put spectrum to use: Rajaraman, Telecom News, ET Telecom (indiatimes.com)

[13] Satellite Communication: Space technologies offer convergence, can put spectrum to use: Rajaraman, Telecom News, ET Telecom (indiatimes.com)

chips for strategic purposes. In 1989, SCL was destroyed in a fire, and it failed to be rebuilt in the last three decades. The upgrade is being planned and funded by the Ministry of Electronics and Information Technology, from the $10 billion incentive package announced in December 2021, to strengthen India's intellectual property rights (IPR) in the semiconductor space.

SCL currently makes 180 nm chips used in defence, space and other applications, that will be upgraded to produce 28-nm chips. The government is trying to rebuild the facilities with support from Taiwanese multinationals such as TSMC and Hon Hai Technology Group (Foxconn), under the Production Linked Incentive (PLI) scheme. The request for proposal (RFP) inviting bids for the modernisation plan, has the cut-off date as October 25.[14]

[14] Govt to spend $1.30 billion to modernise semiconductor laboratory in Mohali - The Economic Times (indiatimes.com)

International Developments

Hacktivists publishes information from Iran's nuclear program

On October 22, hacktivist group "Black Reward" published confidential information on its Telegram channel and on Twitter, that were purportedly stolen from Iran's Atomic Energy Organization. The information includes public and private conversations, construction plans, management, and operational schedules and the "passports and visas of Iranian and Russian specialists" involved in the country's nuclear program. The group had demanded the release of prisoners detained during the ongoing mass protests in Iran, in exchange for not releasing the data.[15]

On October 23, Iran's government issued a statement that "a specific foreign country" was behind the hacktivist group's actions. Iran has been hit by several highly sophisticated hacktivist attacks in the past year, which some experts have said are too advanced to be carried out by hacktivists and are probably the work of Israel. Multiple groups claimed hacks and DDoS attacks under the banner of Anonymous, during the protests.[16]

German cybersecurity chief ousted for Russia ties

On October 18, Arne Schoenbohm, the head of the Federal Cyber Security Authority (BSI), was dismissed following reports of possible ties to Russian intelligence services, with the country on high alert over potential sabotage activities on the country's critical infrastructure by Russia, because of Berlin's support for Ukraine.

The BSI has warned that companies, individuals, and critical infrastructure are at risk of being hit by Russian cyberattacks. Early October the rail network in the north of Germany was temporarily paralysed by "sabotage", possibly by Russia. Important communications cables were cut at two sites, forcing rail services to be halted for three hours and causing travel chaos for thousands of passengers. Moscow is also suspected of being behind explosions last month that set off leaks in the Nord Stream 1 and 2 gas pipelines, which connect Russia to Germany.[17]

[15] Hackers target subsidiary of Iran nuclear agency, demand release of prisoners held in recent protests - World News (wionews.com)

[16] https://www.cyberscoop.com/iran-nuclear-emails-hack-leak-black-reward/

[17] https://www.securityweek.com/german-cybersecurity-chief-sacked-over-alleged-russia-ties

Slovak parliament suspends voting due to suspected cyberattack

European Union countries are increasingly encountering cyber-attacks, as they help Ukraine in the ongoing Russia-Ukraine War. On October 27, the Slovak parliament suspended its session and its voting process, after a suspected cyberattack brought down its IT systems. Local media reported that the parliament session, with 75 bills on the agenda, should reconvene on November 8.

In neighbouring Poland, the website of the upper house of the parliament, the Senate, was down on the same day due to an attack by hackers. The European Commission proposed stepping up measures to protect its critical infrastructure, including digital and energy networks.[18]

Pro-Russian cyberattack affects websites of major US airports

On October 10, websites of 14 major US airports were temporarily brought offline by cyberattacks with Pro-Russian hackers- "Killnet", claiming responsibility for the disruption. The hacktivists apparently support the Kremlin but are not directly linked to government agencies. The distributed denial of service (DDoS) attacks only affected the public-facing websites of the airports, which supply flight and services information and did not affect air traffic control, internal airport communication or other key operations. A similar attack also targeted communication networks in Germany's railway systems, causing massive service disruptions in the northern part of the country.[19]

Chinese Internet Users Lose Access to WeChat App after Protests

After two banners with messages condemning Chinese leader Xi Jinping were hung from a bridge in Beijing on October 13, that began to circulate online, many Chinese were suspended from the inhouse Chinese app "WeChat". Those having clandestine access to Twitter likened the loss of WeChat to "digital death", as WeChat app not only connect family and friends but is used to hail taxis, buy train tickets, pay for groceries, and manage investments. Twitter is blocked in China and only accessible to people there through virtual private networks (VPN), leaving it largely out of reach of Chinese censors.

[18] Slovak parliament suspends voting due to suspected cyberattack, CIO News, ET CIO (indiatimes.com)

[19] https://www.theguardian.com/us-news/2022/oct/10/cyberattacks-disrupt-us-airport-websites

Prior to the Chinese Communist Party Congress-2022 from October 16-22, Chinese authorities had tightened their grip around online discourse to an unusual degree. The country's most popular social-media platforms had been scrubbed of independent or negative content concerning Mr. Xi and many of the country's other top officials, making it essentially impossible to gauge public opinion of the party's leadership. As on October 13, Tencent's customer-services forum on Weibo, a Twitter-like social media platform, was no longer accessible.[20]

The US-China tech war escalates with new export controls

On October 7, the Biden administration announced a new export controls policy on artificial intelligence (AI) and semiconductor technologies, in its bid to slow Beijing's technological and military advances, thus escalating the US-China Tech War. The policy effectively bars any company in the world from sending to China advanced chips, made with US technology, that can be used for AI. The rules block shipments of a broad array of chips for use in Chinese supercomputing systems, with more than 100 petaflops of computing power within a floor space of 6,400 square feet, that could even hit some commercial data centers. Restrictions have also been placed on Semiconductor Manufacturing Equipment (SME). The latest extreme ultraviolet (EUV) technology - available only from the Dutch company-ASML, that helps to manufacture smaller chips (5 nm and below), has been denied to the Chinese.[21]

The policy also prohibits US citizens or green card holders to support the development or production of advanced chips in China, that has forced several global and Chinese technology companies to withdraw such employees and be deprived of their expertise.[22]

On October 13, the US Bureau of Industry and Security (BIS) announced changes to the export administration regulations (EAR), pertaining to certain semiconductor manufacturing items along with expanded controls on transactions involving items for supercomputer and semiconductor manufacturing. The rules named 28 entities in China for which licensing regulations would be required for technology and material transfer.

In December 2021, BIS notified controls on four technologies based on decisions in the Wassenaar Arrangement on Export Controls for Conventional

[20] https://www.wsj.com/articles/WP-WSJ-0000302695

[21] semiconductors: The chips are getting high: US gets its act together in denying China technology - The Economic Times (indiatimes.com)

[22] https://www.reuters.com/technology/us-aims-hobble-chinas-chip-industry-with-sweeping-new-export-rules-2022-10-07/

Arms and Dual-Use Goods and Technologies (WA) plenary meeting in Vienna. Three of these four technologies pertained to the semiconductor ecosystem.[23]

The decision led several firms, including Lam Research and KLA Corporation, to suspend their cooperation with Yangtze Memory Technologies Company (YMTC), for production of its most advanced microchips. It is estimated that China's other large chipmaker, Semiconductor Manufacturing Company (SMIC), will see its growth halved by the restrictions in 2023.[24]

Waivers were however announced on October 13, that allowed major manufacturers including Samsung, Nvidia, Taiwan Semiconductor Company (TSMC) to continue manufacturing in China until September 2023. TSMC is mainly expanding some mature chip production in Nanjing, its most advanced semiconductor production plant in China.[25]

In the face of these sweeping restrictions, China is building more than 30 new fabrication units (fabs) by 2024 - much more than in Taiwan, South Korea, and the US. It was reported on October 22, that China's Ministry of Industry and Information Technology convened a series of emergency meetings with leading semiconductor companies, seeking to assess the damage from such restrictions and pledging support for self-reliance in the critical sector.[26]

The US National Security Strategy-2022 released

On October 12, the US President released "The National Security Strategy-2022" (NSS), that lists the security concerns and challenges of the US and the plans to deal with them. The main thrust of the strategy is that America will focus on competing with China and containing Russia, and it will do so by investing in technologies at home, building a coalition of like-minded states, and modernizing its military. India is mentioned in the NSS in relation to cooperation with democracies and like-minded countries, especially in the context of the Indo-Pacific and Quad.

The Strategy underlines the need for updating the rules of the road for technology, cyberspace, trade, and economics. "Technology is central to today's geopolitical competition and to the future of national security, economy and democracy", it mentions. The need to partner with industry and

[23] semiconductors: The chips are getting high: US gets its act together in denying China technology - The Economic Times (indiatimes.com)

[24] US Tech Curbs Could Halve Growth of China's Top Chipmaker - Bloomberg

[25] US reportedly grants TSMC, Samsung 1-year waiver for chip equipment export to China (digitimes.com)

[26] China Summons Chip Firms for Emergency Talks After US Curbs - The Economic Times (indiatimes.com)

governments in shaping open and transparent technological standards process that enables innovation, growth, and interconnectivity has been emphasised.

The Strategy focusses on securing Cyberspace by working closely with allies and partners, such as the Quad, to define standards for critical infrastructure to rapidly improve cyber resilience and building collective capabilities to rapidly respond to attacks. It aims to deter cyber-attacks from state and non-state actors by responding with all appropriate tools of national power to hostile acts in cyberspace, including those that disrupt or degrade vital national functions or critical infrastructure. With regards to data, it aims to counter the exploitation of American's sensitive data and illegitimate use of technology, including commercial spyware and surveillance technology.

The Strategy professes to promote adherence to the UN General Assembly-endorsed framework of responsible state behaviour in cyberspace, which recognizes that international law applies online, just as it does offline.[27]

Musk makes swift changes after taking over ownership of Twitter

On October 27 Elon Musk completed the $44 billion deal to take over Twitter. His first move was to fire four top executives, including its chief executive Officer, Chief financial officer, general Counsel and its head of legal policy, trust and safety who guided the company's policies on harmful speech, and whose team banned Trump after the January 6 Capitol riot. His takeover is likely to have huge implications for the future of the social media app, with changes to the rules to prevent the spread of hate speech and misinformation.

'Free speech' is a critical part of Musk's agenda as far as Twitter is concerned. But he has promised to advertisers that he does not intend to turn Twitter into a hellscape, and that 'free speech' will remain within the realm of the law.[28]

On October 28, Elon Musk twitted that "Twitter would be "forming a content moderation council with widely diverse viewpoints." No major content decisions or account reinstatements will happen before that council convenes.[29]There has been no mention regarding the prevalence of fake and spam accounts—the issue that was poised to derail the deal. Further, his

[27] Biden-Harris Administration's National Security Strategy.pdf (whitehouse.gov)
[28] Revamping verification to moderation council: Elon Musk's big plans for Twitter so far | Technology News,The Indian Express
[29] https://twitter.com/elonmusk/status/1586059953311137792

approach on free speech may risks causing conflicts with some advertisers, politicians and users who would prefer a more moderated platform.

It was revealed on October 31, that Twitter with roughly 7,500 employees, is drafting plans for broad layoffs, which are expected to reduce engineering positions. The full scale of cuts being discussed is not yet revealed. A working group of advisers, investors and employees from outside Twitter is being set up to help Musk reimagine Twitter. The group is working on a range of initiatives to try to bolster the platform's user experience and revenue.[30]

[30] Twitter Drafts Broad Job Layoffs in Elon Musk's First Week as Owner - WSJ

International Cooperation

India hosts 90th INTERPOL General Assembly

On October 18, the 90th General Assembly Meeting of the International criminal police organisation (INTERPOL) was inaugurated by the Indian Prime Minister in New Delhi. INTERPOL facilitates worldwide police cooperation and crime control across 195 member countries, with different legal frameworks, systems, and languages. The organisation has 90 million records spread across 17 databases.

The meeting discussed how communication, collaboration and cooperation may help to defeat crime, cybercrime, child abuse, corruption, and terrorism, which go beyond conventional geographic borders. The importance of technology like artificial intelligence, and the metaverse for agile policing, to deal with the changes taking place in the cyber threats landscape, were discussed. A proposal was made to carry out detailed research on the challenges likely in the next 35-50 years and bring out a report called World "Policing between 2048 and 2073", which may be reviewed every 5 years.

The Meeting also showcased Indian initiatives to deal with crime and terrorism. The key pillars of criminal justice that form the Inter operable criminal justice system (ICJS) - e-courts, e-prisons, e-forensics and e-prosecution have been linked to Crime and Criminal Tracking Network and systems (CCTNS). A national data base has been created on terrorism, narcotics, and economic offences. The Indian government has established the National Forensic Science University, and the Indian Cyber Crime Coordination Centre (I4C), to combat cyber-crime in a comprehensive manner.[31]

India wins at RRB of the International Telecommunication Union

On October 27, India won the coveted post of a board member at the Radio Regulation Board (RRB) of the International Telecommunication Union (ITU), that would enable the country to effectively work towards spectrum dispute resolutions among countries. India's Representative Revathi Mannepalli won with a record margin of 139 votes out of 180, becoming the first woman candidate for RRB in Asia region and elected for 2023-2026 term.

The ITU is the UN body responsible for telecommunications, radio, satellite and information and communications technology standards setting. While

[31] https://pib.gov.in/PressReleseDetailm.aspx?PRID=1869983

the ITU sets standards that enable global connectivity, the internet itself is governed by a multi-stakeholder approach. The ITU's regulatory board (RRB) deals with satellite and terrestrial spectrum related issues and interference resolutions.[32]

***

[32] International Telecommunication Union: India's ITU win a diplomatic success, Telecom News, ET Telecom (indiatimes.com)

DPG

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

www.delhipolicygroup.org