Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

JANUARY 2022

Volume III, Issue 1 | January 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 1
January 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 1
January 2022

Contents

Abstract

The onset of 2022 has seen global geo-political tensions impacting the cyber space. Adversaries continue to invade Indian cyberspace, signalling the continuing shift of conflicts to the grey zone. The fourth quarter of 2021 saw an all-time peak in cyber-attacks, particularly after the discovery of Log4j vulnerabilities.

Semiconductor supply chains in India are being strengthened with several programs including "Chips2Startup" and "design linked incentives", to implement the $10 billion incentive scheme for chip manufacturing announced last month. The government released a 5-year roadmap for the electronics sector titled "$300 bn Sustainable Electronics Manufacturing & Exports by 2026" and "National Strategy on Blockchain". 5G is likely to be rolled out by private telecom players in 2022-23.

The Global Risk Report 2022 released by the World Economic Forum (WEF) warned that geopolitical rifts around digital sovereignty have hindered potential cross-border collaboration to undertake "established" or "effective" international risk mitigation efforts in areas of cross border cyberattacks, mis-information and artificial intelligence.

Geopolitical contestation over Ukraine have turned cyberspace as a battle ground among adversaries, heralding "Hybrid Warfare" as a precursor to kinetic war. Cyberattacks are also being witnessed against the International Committee of the Red Cross (ICRC), which have compromised personal data and confidential information on more than 515,000 highly vulnerable people.

In the US, the telecom and aviation industry differed over the rollout of 5G cellular networks near airports, which could interfere with legacy navigation systems of aircraft. A temporary solution has avoided an immediate crisis, but a long-term solution would require time to deploy retrofitted aircraft altimeters with new standards.

To reduce the risk of future supply-chain disruptions, the US, Europe and other countries, including India, are devising massive subsidy and incentive packages. In the US alone, the semiconductor industry has announced nearly $80 billion in new investments through 2025. In response to recent high profile attacks, the US administration extended its critical infrastructure cybersecurity initiative to the water and wastewater sectors, besides the electric grid and natural gas pipelines.

India hosted the first Colombo Security Conclave Virtual Workshop on "Developing Regional Cyber Security Capabilities on Defensive operations, Deep/Dark Web handling and Digital Forensics" on January 10-11.

National Developments

Pakistani misinformation campaigns against India

Twice during this month, the Indian Government invoked its emergency powers under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, to ban social media accounts operating from Pakistan and spreading "anti-India disinformation". On January 12, it ordered a ban on 73 Twitter handles and 4 YouTube channels for circulating a fake Cabinet meeting video.[1] Again, on January 21, it ordered a ban on 35 YouTube channels, two websites, two Twitter accounts, two Instagram accounts and one Facebook account. The channels reportedly were responsible for spreading "anti-India" content with a focus on the Indian armed forces, Jammu and Kashmir, India's foreign relations, separatist ideology and public order. The fake and inflammatory content was deemed to be directed against the sovereignty of the country.[2]

Cyberattacks peaked in the last quarter of 2021

In India, there have been on average 1803 weekly attacks in 2021, which is a 24 per cent increase from 2020. On January 11, it was reported that the fourth quarter of 2021 saw an all-time peak in weekly cyber-attacks, with over 900 attacks per organisation.[3] The peak also came after the discovery of Log4j vulnerabilities, that disrupted servers of major tech giants such as Microsoft, Amazon, and Apple. Globally, Europe saw the highest percent increase in cyberattacks year over the past year. A report by the Check Point Research points out that "attacks penetrate networks by leveraging known vulnerabilities which are not patched".[4]

Blockchain and quantum computing for data security

Aadhaar, the national identity platform, has become the mainstay of financial inclusiveness. Over five crore Aadhaar authentications are taking place per day and over 40 crore last-mile banking transactions are being done every month through the Aadhaar-enabled payment system (AePS). As on December 31, 1.32 billion Aadhaar cards had been generated.[5] However, media reports continue

[1] MeitY suspends 73 Twitter handles, 4 YouTube channels for circulating fake Cabinet meeting video, Government News, ET Government (indiatimes.com)
[2] Centre orders ban on 35 Pakistan-based YouTube channels - The Hindu
[3] After Log4J flaw, cyberattacks peaked towards the end of 2021: Check Point Research (msn.com)
[4] https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/
[5] Monthly achievements month of December 2021.pdf (meity.gov.in)

to emerge from time to time that the Aadhaar data is being compromised, for various reasons.

On January 12, it was reported that the Unique Identification Authority of India (UIDAI) is looking at solutions that can enable 'partial authentication', on need-to-know basis, to secure Aadhaar data. The Aadhaar-issuing body is exploring the possibilities for the use of blockchain and quantum computing, for decentralised or quantum resilient security solutions, for its 'Aadhaar 2.0' vision. It is seeking industry feedback on faster automated biometric matching solutions with a primary focus on the security of the ecosystem.[6]

Efforts to make India the next Semiconductor hub

In line with the objectives and visions of the National Policy on Electronics (NPE-2019), an umbrella program "Chips to Start-Ups" (C2S) has been initiated to strengthen the semiconductor supply chain. On January 16, the nodal ministry has sought applications under the C2S Programme, which aims to train 85,000 engineers in various aspects of chip design and work out prototypes over a period of five years.[7] The programme would be implemented at 100 academic institutions/R&D organisations across the country in collaboration with start-ups and MSMEs.[8]

Further, on January 17, the nodal ministry released the framework for implementing the Design Linked Incentive (DLI) Scheme, announced in December 2021. There are three components to the Framework.

Under the Chip Design infrastructure support, C-DAC will set up the India Chip Centre to host the state-of-the-art design infrastructure, post-silicon validation and facilitate its access to supported companies. Under the Product Design Linked Incentive component, reimbursement of up to 50 per cent of the eligible expenditure, subject to a ceiling of Rs 15 crore per application, will be provided as fiscal support. Under the Deployment Linked Incentive component, an incentive of 6 per cent to 4 per cent of net sales turnover will be given over five years subject to a ceiling of Rs 30 Crore, to applicants whose semiconductor designs for Integrated Circuits (ICs), Chipsets, System on Chips (SoCs), etc. are deployed in electronic products.

[6] UIDAI exploring usage of blockchain and quantum computing for 'Aadhaar 2.0': CEO Saurabh Garg, Government News, ET Government (indiatimes.com)
[7] https://www.meity.gov.in/content/call-proposal-chips-startupc2s-programme
[8] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1790350

The scheme will adopt 100 domestic companies, start-ups and MSMEs. A dedicated portal has been made available – www.chips-dli.gov.in - for inviting Online applications from January 1, 2022 to December 31, 2024.[9]

5G trials and the hurdles for its early launch

While 5G trials are being conducted across the country, the Finance Minister, in her budget speech on February 1, stated that the required spectrum auction will be conducted in 2022 for the rollout of 5G mobile services within 2022-23, by private telecom providers.[10]

Before the roll out of 5G, many contentious issues need to be resolved. On January 11, the Telecom Regulatory Authority of India (TRAI) informed the Department of Telecommunications (DoT) that it would submit 5G pricing recommendations by March, based on the industries' views on topics related to quantum of spectrum to be auctioned off, band plan, block size, and conditions for auction of spectrum in new bands.

Subsequently, on January 12 the Satcom Industry Association-India (SIA) submitted to TRAI that bifurcating satellite bands for the upcoming 5G auction is likely to incur a massive $184.6 billion loss to the country. It urged TRAI to limit the inclusion of mm Wave spectrum in any 5G auction to the internationally harmonised 24-27.5 GHz spectrum.[11] The centre of controversy is the 28 GHz band between satellite service companies and terrestrial network operators.

On January 16, the telecom body - the Cellular Operators Association of India (COAI) - maintained that the 28 GHz (Ka band) should be reserved for commercial 5G services, while the newly created Indian Space Association (ISpA) has suggested that in the 24-27.5GHz band, there is adequate capacity for four major mobile terrestrial incumbents in India and hence retaining 27.5 to 28.5 GHz with the space sector will not in any way inhibit the propagation of 5G.[12]

Raising another controversial issue regarding merits of auction vis-à-vis administrative allocation of spectrum, on January 17 Reliance Jio urged TRAI

[9] semiconductor: Ministry of Electronics, IT invites applications from domestic companies for semiconductor chip design, Telecom News, ET Telecom (indiatimes.com)
[10] Budget 2022 LIVE: Digital rupee, 5G, crypto tax among major announcements | Hindustan Times
[11] Bifurcating satellite bands for 5G may cost India $184 bn: SIA-India | Business Standard News (business-standard.com)
[12] Reserving 28GHz frequency band for satellite will not discourage propagation of 5G: Space group, Telecom News, ET Telecom (indiatimes.com)

to auction all spectrums for broadband usage from space services, in line with trends gaining ground globally. It cited examples of Brazil, Saudi Arabia, Mexico and Thailand. Jio contends that such a move would be in line with the Supreme Court's 2012 verdict that had backed allocation of airwaves through transparent auctions alone.[13]

To address all technical issues for early roll out of 5G, on January 4, the government set up six academia-driven task forces, to work on multi-platforms for next generation networks, spectrum policy, multi-disciplinary innovative solutions, and devices respectively. The task force on international standards is led by the Telecommunications Standards Development Society, India. Immediate deliverables have been mandated by March 31, that have included mapping of 6G activities and capabilities worldwide, and a white paper on India's competencies.[14]

In another development, the Digital Infrastructure Providers Association (DIPA), has on January 8 hailed the National Master Plan "Gati Shakti'' as very significant for the telecom sector on various fronts, such as a unified portal for approvals of infrastructure projects, cross-sector collaboration with utilities (water, gas, electricity, etc.) for Right of Way (RoW) permissions, and availability of land/properties for deploying infrastructure. These initiatives would also address software and security of infrastructure to ensure a robust and secure state-of-the-art telecommunication infrastructure.[15]

Early roll out of 5G also requires infusion of funds. While the administrative reforms by the government have helped the telecom sector financially, investments by industries is a positive development. On January 28, Airtel and Google entered into a "long-term, multi-year agreement" to accelerate the growth of India's digital ecosystem. As part of this partnership, Google plans an investment of $1 billion, over a period of five years. Under the larger strategic goals of the partnership, both companies will develop India-specific 5G use cases and other standards, with cutting-edge implementations. Airtel is already using Google's 5G-ready network platforms, and plans scaling up Google's network Virtualisation solutions.[16] Google has also invested in Reliance Jio a

[13] Reliance: Jio tells Trai auction of spectrum for broadband-from-space services gaining traction globally - The Economic Times (indiatimes.com)
[14] Vodafone Idea: Telcos want to be included in 6G task forces constituted by DoT: Report, Telecom News, ET Telecom (indiatimes.com)
[15] Gati Shakti National Master Plan: Gati Shakti National Master Plan provides boost to digital infrastructure: DIPA, Telecom News, ET Telecom (indiatimes.com)
[16] Bharti Airtel: Google to invest up to $1 billion in Airtel; to co-create India-specific 5G use cases, Telecom News, ET Telecom (indiatimes.com)

sum of $4.5 billion, while it has backed more than a dozen startups in India through its accelerator programme.

India releases 5-year road map for electronics manufacturing

"Make in India" is the key to cyber security, besides saving multi-billion dollars in imports. With that objective, on January 24, the Ministry of Electronics and Information Technology, in association with the India Cellular & Electronics Association (ICEA), released a 5-year roadmap and Vision Document for the electronics sector titled "$300 bn Sustainable Electronics Manufacturing & Exports by 2026." Mobile manufacturing, which is expected to cross US$100 billion in annual production, is slated to constitute nearly 40% of this ambitious growth, while exports are expected to increase from a projected US$15 billion in 2021-22 to US$120 billion by 2026.

This vision document recommends that for achieving the target, the focus must be on building of scale through incentives, removal of cost disabilities, and growth and diversification of global value chains. The documents also calls for review of existing policies within the next 1,000 days, including stability in import tariffs, decrease in import tariffs for components with no manufacturing base in India, development of skill sets, and encouraging major foreign manufacturers to set up components ecosystems in India.[17] Towards realising the goal of a self-reliant India, it also details the importance of the key role Indian champions will play in addition to global companies – both of whom are already part of the Production Linked Incentives (PLI) Schemes, that aggregate to nearly US$17 billion over the next 6 years.[18]

Indian government launches national strategy on blockchain

In December 2021, the government released a 'national strategy on blockchain' which aims to evolve a trusted digital platform for providing e-governance services using blockchain and the development and implementation strategies for a national blockchain platform covering the technology stack, legal and regulatory framework, standards development, collaboration, human resource development and potential use cases. The multi-institutional framework includes C-DAC for research and development, NIC and NICSI for hosting the national-level blockchain infrastructure, while the national e-governance division will handle the implementation of projects undertaken by various

[17] https://www.thehindu.com/business/india-can-make-300-bn-electronics-by-2026/article38320653.ece
[18] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1792189

organisations. Implementation of the blockchain strategy would enhance security, trust and the ability to ensure tamper-evident transactions.[19]

[19] MeitY releases national strategy on blockchain for its adoption in government systems (yourstory.com)

International Developments

Global Risk Report 2022 by WEF

On January 11, the World Economic Forum (WEF) released the Global Risk Report 2022, that warned about the ongoing and upcoming challenges created by cyber fraudsters. According to the report, cyber security and space remain among the most emerging risk sectors to the global economy, besides the ongoing COVID-19 pandemic. It contends that inequalities in digital security will only widen with the advent of internet 3.0 and the metaverse.

According to the report, while the growth in value of digital commerce is set to rise to $800 billion by 2024, 95% of cyber security issues will be caused by human error. Malware and ransomware attacks have boomed, while the rise of cryptocurrencies makes it easy for online criminals to avoid traceability. Linkages of criminals to government agencies are leading to open cyberwarfare.

The report points out that geopolitical rifts have hindered potential cross-border collaboration, and given the geopolitical tensions around digital sovereignty, "cross-border cyberattacks and misinformation" and "artificial intelligence" were among the areas with the least "established" or "effective" international risk mitigation efforts.

Capability building is a major issue highlighted in the report. There is a gap of more than 3 million cyber professionals worldwide, who can provide cyber leadership, test and secure systems, and train people in cyber hygiene. The report has concluded that unless digital trust is improved with intentional and persistent trust-building initiatives, the digital world will continue to drift towards fragmentation.[20]

On January 18, the Indian PM virtually delivered a 'State of the World' special address at the World Economic Forum's Davos Agenda, highlighting Indian achievements and a wish-list for reforms in multilateral bodies. He mentioned that "India has deregulated areas like Drones, Space, Geo-spatial mapping and has brought reforms in the outdated telecom regulation related with the IT and

[20] WEF_The_Global_Risks_Report_2022.pdf (weforum.org)

BPO sectors ".[21] On January 21, WEF announced that its annual meeting will be held in person at Davos from May 22-26.[22]

Cyberspace becomes a battleground over geopolitical contestations

On January 14, cyberattacks targeted more than 70 Ukrainian government websites, including the foreign ministry, the cabinet of ministers and the security and defence council, among others. On January 16, Ukraine attributed the 'wiper' and 'defacement' cyberattacks to Belarussian threat actor UNC1151, which is also allegedly involved in disinformation campaigns in Europe. Linkages have also been found with a group "Sandstorm" allegedly tied to Russian intelligence. Belarus is a close ally of Russia, and Ukraine has allegedly served as a testing ground for Russian cyberweapons, including attacks on power grids in 2016 and NotPetya ransomware attacks in 2017 that had targeted Ukrainian businesses and caused more than $10 billion in damage globally.[23]

These attacks prompted a response from NATO. On January 14, NATO Secretary-General Jens Stoltenberg said that the alliance will provide "strong political and practical support" to Ukraine in light of the cyberattacks. Moscow has denied its involvement in these cyberattacks.[24]

In the wake of heightened tensions with Ukraine and increased presence of Russian troops in Belarus, the "Belarusian Cyber Partisans", a network of activist hackers that aims to overthrow Belarusian President Alexander Lukashenko's regime, announced on January 24, on Twitter and Telegram, that it had targeted the state-owned Belarusian Railway and encrypted the majority of the company's servers, databases and workstations, demanding that the government bar the presence of the Russian military in Belarus and release 50 political prisoners needing medical attention.[25] It is generally unusual for non-state actors to deploy ransomware for political objectives. More such attacks are expected against either camp, signalling the onset of "Hybrid Warfare".

[21] https://mea.gov.in/press-releases.htm?dtl/34755/PM_delivers_State_of_the_World_special_address_at_the_World_Economic_Forums_Davos_Agenda
[22] World Economic Forum to hold 2022 annual meeting in Davos in May - The Economic Times (indiatimes.com)
[23] https://www.securityweek.com/microsoft-uncovers-destructive-malware-used-ukraine-cyberattacks
[24] Massive cyberattack hits Ukrainian govt's websites as West warns on Russia conflict - World News (indiatoday.in)
[25] https://www.bloomberg.com/news/articles/2022-01-24/hackers-say-they-breached-belarusian-rail-to-stop-russian-troops

Russia and Ukraine dismantle hacker groups

In a rare gesture to de-escalate risks of damaging cyber-attacks, both Russia and Ukraine have acted on hackers. On January 14, Russia dismantled the notorious ransomware gang REvil, as the Russian Federal Security Service (FSB) arrested more than a dozen people affiliated with the group and searched over 25 addresses. The FSB acted on the request of American law enforcement and the men arrested face up to seven years in prison if convicted. The FSB also seized 426 million roubles ($5.6 million) in a raid against 14 members of the group, along with more than $600,000 worth of cryptocurrency and 20 luxury cars. The FSB said that REvil hackers with Russian citizenship will not be extradited to the US.[26] The announcement came on the same day that Ukrainian government sites were hit by hackers in an attack that Kyiv linked to Moscow.

Simultaneously on January 13, Ukrainian authorities announced the arrest of several individuals who are allegedly members of a major cybercrime group. According to the Security Service of Ukraine and the country's Cyber Police, the arrests are the result of an operation conducted in cooperation with law enforcement agencies in the United Kingdom and the United States. The suspects allegedly carried out ransomware attacks against more than 50 companies in the United States and Europe, and made over $1 million by encrypting their files and asking for a ransom.[27]

North Korea hit by cyberattacks

On January 26, a researcher based in Britain reported that North Korea's internet appeared to have been hit by a second wave of outages, possibly caused by a distributed denial-of-service (DDoS) attack, that tries to flood a network with unusually high volumes of data traffic. A similar incident was observed on January 14 for about six hours, coming a day after North Korea conducted its fifth missile test.[28] The attack targeted web servers of the Air Koryo airline, North Korea's ministry of foreign affairs, and Naenara, the official portal for the North Korean government.[29] The extent of damage is unknown as Internet access is limited in North Korea.

[26] https://www.ibtimes.co.in/russian-court-charges-8-revil-ransomware-hackers-behind-us-attacks-details-844787
[27] https://www.securityweek.com/ransomware-group-targeted-over-50-companies-dismantled-ukraine
[28] N.Korea fires cruise missiles amid tension over lifting nuclear moratorium | Reuters
[29] https://www.reuters.com/world/asia-pacific/nkorean-internet-downed-by-suspected-cyber-attacks-researchers-2022-01-26/

Hackers target the International Red Cross

On January 19, the International Committee of the Red Cross announced that it was the victim of a sophisticated cyber security attack that compromised personal data and confidential information on more than 515,000 highly vulnerable people, including those "separated from their families due to conflict, migration and disaster". It said the information originated in at least 60 Red Cross and Red Crescent chapters around the world. The breach targeted an external contractor in Switzerland that stores data for the humanitarian organisation, and there was no indication the information had been publicly shared or leaked.[30]

Rift over 5G deployment between American regulators

The U.S. telecom companies and airlines had a face-off over the rollout of 5G cellular networks using a segment of the radio spectrum that could cause interference with legacy navigation systems of aircraft. While the telecom regulator-FCC contends that the 5G deployment can safely co-exist with aviation technologies, the aviation regulator-FAA has warned of catastrophic consequences.

On January 18, telecom operators agreed to restrict 5G near airports to avoid potential interference with altimeters on planes. The temporary solution will keep C-band 5G two miles away from potentially affected airports. Even with the airport restriction, a number of international airlines, including Air India, had canceled flights to the United States, though some of those flights were later restored.

Technically, 5G interference problems can be solved with new or retrofitted aircraft altimeters with new standards, but they are not scheduled to be released for review until October. An early resolution of the long pending problem will be expected by the world community.[31]

Semiconductor chip shortage spurs industries to invest

To reduce the risk of future supply-chain disruptions, the US, Europe and other countries, including India, are devising massive subsidy and incentive packages, that have spurred global semiconductor companies to invest and expand. In the US alone, the semiconductor industry has announced nearly

[30] Red Cross: Hack exposes data on 5,15,000 vulnerable people - The Hindu BusinessLine
[31] How 5G Clashed With an Aviation Device Invented in the 1920s - The New York Times (nytimes.com)

$80 billion in new investments through 2025.[32] The US administration has been working to pass legislation which will provide $52 billion to catalyse more private-sector investments.

On January 21, Intel announced an investment of $ 20 billion in two new chip factories in Ohio, that could eventually grow to accommodate eight FABs, with spending potentially reaching around $100 billion over the next decade. On January 13, the Taiwan Semiconductor Manufacturing Co. (TSMC) said it would increase its investment to boost production capacity by up to 47% this year, by setting a capital expenditure budget of $44 billion as demand continues to surge amid a global chip crunch. More than seventy percent of the spending would be towards advanced manufacturing processes, with plans to open plants in Arizona and in Japan in the next five years.[33]

Simultaneously, on January 10, the South Korean memory chip maker SK-Hynix, formed a SK ICT Alliance with QUALCOMM and two other South Korean subsidiaries to jointly develop and invest in information and communication technologies and create global market opportunities. They plan to create and run a 1 trillion won ($830 million) fund this year to invest in the fields of AI, metaverse, chips and block chain technologies.[34] Last year, Samsung said it would spend more than $205 billion over the next three years, with chip-making a priority, and unveiled a $17 billion investment in Texas.[35]

Crypto currency classification poses global dilemma

Regulators across the globe are divided on how to treat decentralised virtual currencies, which are seen posing a risk to financial stability and impacting cross-border transactions. The dilemma remains whether to treat crypto currency as an asset, property, or legal tender.

While El Salvador has recognised Bitcoin as legal tender, many countries, including China, have completely banned crypto. Several other countries have banned their banks from dealing in crypto directly or indirectly and barring crypto exchanges.

The Indian Finance Minister announced on February 1 that a Central Bank Digital Currency (CBDC), the Digital Rupee, using blockchain and other

[32] https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/21/fact-sheet-biden-harris-administration-bringing-semiconductor-manufacturing-back-to-america-2/
[33] TSMC to Invest Up to $44 Billion in 2022 to Beef Up Chip Production - WSJ
[34] qualcomm: SK Hynix to diversify chip biz, collaborate with Qualcomm, Telecom News, ET Telecom (indiatimes.com)
[35] https://www.wsj.com/articles/intel-to-invest-at-least-20-billion-in-ohio-chip-making-facility-11642750760

technologies, will be introduced in 2022-23, while imposing a 30% tax on virtual digital assets.[36]

On January 20, the Bank of Russia proposed to ban the issuance, mining and circulation of cryptocurrencies in Russia in order to alleviate the dangers caused by the proliferation of cryptocurrencies. It sought to ban the issue and organisation of circulation of crypto-currencies on the territory of the Russian Federation and establish liability for violating this ban.[37] Meanwhile, the US administration is preparing to release an initial government-wide strategy for digital assets in February 2022, and task federal agencies with assessing the risks and opportunities that they pose.

International Organisations like the IMF and WEF have also urged that regulation needs to be on the global agenda, though crypto can help make cross-border payments efficient and improve financial inclusion. On January 25, the International Monetary Fund (IMF), cited the recent volatility of Bitcoins and urged El Salvador to strip Bitcoin of its status as a legal tender because of large risks to financial stability, consumer protection and fiscal liabilities. Since last November, Bitcoin's decline has wiped out more than $600 billion in market value, and over $1 trillion has been lost from the aggregate crypto market.[38]

The IMF has long warned against adopting highly speculative crypto assets as national currency, primarily because the privately issued tokens bypass authorities and central banks tasked with preserving economic and currency stability. It suggests that as enforcement of bans remain difficult, countries should look towards establishing robust regulatory frameworks.

US expands critical infrastructure partnership to the Water sector

There have been several recent attacks in the US on water and sewage systems since 2019, including one in August 2021 that involved the 'Ghost' ransomware being deployed against a facility in California, an attack in July 2021 trying to damage a wastewater facility in Maine, and against a Nevada water treatment plant in March 2021. On January 27, the US administration announced "the Water and waste-water Sector Action plan" that will extend the Industrial Control Systems (ICS) Cybersecurity Initiative to the water sector. Post attacks

[36] Digital rupee to be introduced by the RBI: Budget 2022 - The Economic Times (indiatimes.com)
[37] Central Bank seeks ban on issuance, mining, circulation of cryptocurrencies in Russia - Business & Economy - TASS
[38] Crypto crash: Crypto crash erases more than $1 trillion in market value - The Economic Times (indiatimes.com)

on the US high-profile critical infrastructures, the US administration had established ICS initiatives for the electric grid and natural gas pipeline subsectors. The plan calls for partnership with the private sector and municipal owners and operators of that infrastructure, with information sharing and technical support over the next 100 days. The Plan was developed in close partnership with the Environmental Protection Agency (EPA), the Cybersecurity and Infrastructure Security Agency (CISA), and the Water Sector Coordinating Council (WSCC).[39]

It can be hoped that the much-awaited Indian National Cyber Security Strategy would also consider the water sector as part of its Critical Infrastructure Protection plan.

[39] Fact Sheet: Biden-Harris Administration Expands Public-Private Cybersecurity Partnership to Water Sector | The White House

International Cooperation

India hosts two-day Virtual Cyber Security Conclave

India hosted the first Colombo Security Conclave Virtual Workshop on "Developing Regional Cyber Security Capabilities on Defencive operations, Deep/Dark Web handling and Digital Forensics" on January 10-11. Delegates from Member and Observer States of the Colombo Security Conclave (CSC) including Sri Lanka, Maldives, India, Mauritius, Seychelles, and Bangladesh participated in the workshop. Participants shared their experiences in dealing with cyber security threats and agreed to cooperate on cyber security and identify key deliverables.[40]

On August 4, 2021, all member countries of the Colombo Security Conclave had agreed to cooperate on Maritime Safety and Security; Terrorism and Radicalisation; Trafficking and Organised Crime; and Cyber Security and Protection of Critical Infrastructure.[41]

India-US Homeland Security Dialogue on Cyber security

On January 12, India and the US reviewed their ongoing cooperation in counterterrorism, cyber security, critical infrastructure protection, global supply chains security and other issues as part of the Homeland Security Dialogue, which was held in virtual mode. Existing sub-groups will meet in the coming months to deliberate and explore how ongoing cooperation can be strengthened further.[42]

US DOD conducts multinational cyber exercise

The U.S. Cyber Command conducted its largest multinational cyber exercise 'CYBER FLAG 21-1' last month, to enhance collective defence skills of cyber operators from 23 countries, including Canada, Denmark, Estonia, France, Germany, Lithuania, Norway, the Netherlands, Poland, Sweden, the United Kingdom and others. The exercise supported the objectives of strengthening defensive cyber operation of the international community, and sought to improve their capabilities to identify, synchronise, and respond to malicious cyberspace activities.[43]

***

[40] https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1789124
[41] https://www.thestatesman.com/india/india-hosts-security-conclave-cooperation-regional-cyber-security-capabilities-1503037885.html
[42] https://www.republicworld.com/india-news/general-news/india-and-us-discuss-various-key-issues-during-virtual-homeland-security-dialogue-articleshow.html
[43] Dept. of Defense's largest multinational cyber exercise yet focuses on collective defense > U.S. Cyber Command > News

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

www.delhipolicygroup.org