Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

DECEMBER 2022

Volume III, Issue 12 | December 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 12
December 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 12
December 2022

Contents

Abstract

The Ransomware attack on India's premier health care systems has been a shake up call for its cyber security establishment. The breach has occurred despite public health being recognised as a critical information infrastructure, under the IT Act section 70.

India is the largest 'connected' nation in the world with its userbase adding up to 1. 2 billion, by the proliferation of 5G and Fibre optics network.[1] It is also exploring the Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India to improve the connectivity further.

Indian owned companies like the Vedanta Group and Tata sons are collaborating vigorously with foreign expertise to establish semiconductor manufacturing plant. The draft Digital Personal Data Protection Bill 2022 is undergoing public consultation before finalisation.

On the international front, Taiwan's cyber warfare capabilities have been highlighted, that are being built to confront China in the foreseeable conflict. Taiwan has built the Information Communication Electronic Force Command (ICEF) over 5 years by bringing together communication, cyber, and electronic warfare units for the task.

The US Cyber Command has revealed that it had conducted full spectrum Cyber operations against Russia, Iran, and other proxy actors to protect its critical systems. The US has accelerated its efforts to 'onshore' and 'friend-shore' manufacturing of semiconductor, while it continues to impose curbs for advanced technologies to China, which have implications for global technological leadership and geopolitics.

The European Commission has launched the draft 'adequacy decision' for the EU-US Data Privacy Framework, that assesses the US legal framework that provide adequate safeguards for cross border data flows.

A practical seminar on "Securing the Cyberspace Frontiers", with SCO's Regional Anti-Terrorists Structure (RATS) was conducted by India, with a special focus on examining and deliberating on issues related to misuse of internet by Terrorists, Separatists and Extremists (TS&E).

[1] https://pib.gov.in/PressReleasePage.aspx?PRID=1882603

National Developments

AIIMS ransomware attack galvanises efforts of security agencies

The ransomware attack on AIIMS on November 23, that led to the encryption of approximately 1.3 terabytes of data, has galvanized security agencies to restore its data; investigate origin, intent, extent of the attacks; and measures taken to prevent a recurrence.[2] It is suspected that the hackers are from Hong Kong and Henan in China.

While a case of extortion and cyber terrorism was registered by the Intelligence Fusion and Strategic Operations unit of the Delhi police, it has sought the IP address of suspected Chinese hackers from Interpol. On December 19, a separate probe has been initiated by the National Investigation Agency (NIA) and the Indian Computer Emergency Team (CERT-in), the country's nodal cybersecurity agency.

The collapse of AIIMS digital infrastructure has brought into focus the need to approve the long pending draft National Cyber Security Strategy and to expand the remit of Cyber Crisis Management Plan across all sectors of critical information infrastructure. The strategy would help to operationalise the National Cyber Coordination Centre (NCCC), with delineation of responsibilities. Besides, basic cyber hygiene like using strong passwords, having multi-factor authentication, and regular periodic audits of all systems will help to provide a resilient cyberspace.[3]

Efforts and challenges for 5G roll out

India aspires to be the largest 'connected' nation with a user base of 1.2 billion, with proliferation of 5G and penetration of rural broadband connectivity. As on November 26, Telecom Service Providers (TSPs) have commenced providing 5G services in 50 towns, with trusted network equipment as mandated under the National Security Directive on Telecommunication Sector (NSDTS).[4]

On December 19, the Department of Telecommunications (DoT) has initiated a process to identify 5G spectrum bands, that can be administratively allocated to companies for rolling out private networks, intended for non-public use.[5]

[2] Tharoor raises AIIMS cyber attack in Lok Sabha, demands urgent measures | Latest News India - Hindustan Times

[3] critical-infra-organisations-must-upgrade-security-to-avoid-aiims-like-attacks-say-experts/articleshow/96200913.cms

[4] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1883481

[5] 5G: DoT looks to identify spectrum bands to allocate for private 5G network, Telecom News, ET Telecom (indiatimes.com)

More than 20 companies have applied for direct allocation of spectrum, to offer private 5G network as a service to enterprises through the network slicing capability.

There are several other efforts including expansion of submarine cable, streamlining of Rights of Way (ROW) approvals and inclusion of millimetric waves for early roll out of 5G.

The global extensive network of submarine communication cables that traverses the maritime zones of several countries, are critical to the data driven economy. India has around seventeen submarine cables terminating at fourteen distinct cable landing stations (CLS). But there is no Indian marine service provider available to support the submarine maintenance activities in and around Indian waters. Dependency on foreign service providers involves delayed mobilization time.[6]

On December 23, the Telecom Regulatory Authority of India (TRAI) has issued the Consultation Paper on 'Licensing Framework and Regulatory Mechanism for Submarine Cable Landing in India'. The paper intends to promote domestic submarine cables and terrestrial connectivity between differently located Cable Landing Stations in India. Written comments on the Consultation Paper are invited from the stakeholders by January 20 and counter-comments, if any, by February 3.[7]

The Right of Way (ROW) - clearing passage for installation of telecom infrastructure - is a big challenge to 5G rollout. On December 5, a fresh protocol was laid out to approve ROW across all states. However, several states are still not on board.[8]

On December 16, the Global System for Mobile Communications Association (GSMA), representing Indian telecom players, has urged Indian authorities to release 6 GHz spectrum band for 5G services for expansion in urban areas. 6 GHz plays a core role in delivering 5G networks all over the world. But in India, 6 GHz is partly used for satellite operations by the Indian Space Research Organisation (ISRO) currently and it may be difficult for its release for 5G network.[9]

[6] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1886159
[7] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1886159
[8] 5G rollout: Big right of way delays in opposition-ruled Tamil Nadu, Kerala and Bihar, Telecom News, ET Telecom (indiatimes.com)
[9] Reliance Jio: Telcos seek 6 GHz spectrum band for 5G expansion, Telecom News, ET Telecom (indiatimes.com)

Efforts to build semiconductor ecosystem

India has offered $ 10 Billion as incentives to manufacture semiconductor chips locally. However, chip fabs require a long lead time, stable electric supply, and a skilled workforce. Some Indian companies with support from the government, have formed conglomerates to meet the challenges.

On December 9, the Indian Parliament was informed that the government has modified the Semicon India programme, in view of the aggressive incentives offered by developed countries, and limited number of companies owning the advanced node technologies. The modified programme aims to provide financial support to companies investing in semiconductors, display manufacturing and design ecosystem. The government has also approved modernisation of Semi-Conductor Laboratory at Mohali as a brownfield Fab.[10]

It was reported on December 13, that the Vedanta Group has formed a conglomerate with Taiwan's Hon Hai Technology Group (Foxconn) to build a $20 billion semiconductor fabrication plant, in the Dholera area of Gujrat state. The Foxconn-Vedanta deal would represent the largest corporate investment in India and its first privately owned fab.[11]

On December 9, It was reported by Nikkei Asia, that Tata sons have decided to form a conglomerate to invest $90 Billion over 5 years, to look into the possibility of launching an upstream chip fabrication platform, that is technologically challenging as compared with downstream process of assembly and testing.[12]

India launches pilot of retail Digital Currency

On December 1, India launched the pilot of e-rupee digital currency (e₹-R) in the retail segment as part of the Central Bank Digital Currency (CBDC), issued and backed by the RBI. CBDC is expected to make faster settlement, lower cost of cross-border transactions, and reduction in currency printing. However, concern around privacy, anonymity, data integrity and the resultant cyber-attacks may remain a challenge. China, Singapore, France, Canada, Saudi Arabia, Uruguay, and the United Arab Emirates are among the countries

[10] Semicon India: Govt focused on building semiconductor ecosystem; 4 schemes introduced under Semicon India programme: Minister, Government News, ET Government (indiatimes.com)
[11] India's Manufacturing Push Takes an Audacious Gamble on Chips - WSJ
[12] Tata to enter chip production in India, says chairman - Nikkei Asia

conducting CBDC pilots, with more than 100 CBDCs in research or development stages.[13]

Digital Personal Data Protection Bill under review

The draft Digital Personal Data Protection Bill 2022 (DPDP) is under review. It was brought out during consultations on December 1, that representatives from the National Association of Software and Services Companies (NASSCOM) sounded satisfied with the provision that permits data storage in approved secure geographies. Again, on December 23, consultation with over 200 stakeholders brought out various suggestions related to different clauses of the Bill including the penalty regime for data fiduciaries, regarding obtaining parental consent for children, cross border data flows and about consent managers.[14]

The draft DPDP has proposed an exemption only for government-notified data fiduciaries and data processing entities, to access to personal data only in exceptional circumstances as notified, to allay apprehensions of indiscreet violation of privacy by government agencies.[15]

[13] Digital Currency: Explained: Decoding e-rupee and whether India is ready to transact in digital currency - The Economic Times (indiatimes.com)
[14] https://www.pib.gov.in/PressReleasePage.aspx?PRID=1886126
[15] India's new data protection bill gets Big Tech, startup support - Nikkei Asia

International Developments

Taiwan's Cyber Capabilities being built for future conflict

While China is recognised for its aggressive cyber campaigns, Taiwan's cyber capabilities are often overlooked. A blogpost published by the CFR on December 7, brought out vulnerabilities faced by Taiwan cyberspace including denial of its internet and disruption of its submarine cables. To meet military challenges across the strait, its cyber offensive capabilities have been developed over the last 5 years.

In 2017, Taiwan established the Information Communication Electronic Force Command (ICEF) that brought together communication, cyber, and electronic warfare units under one organisational authority. The cyber warfare wing is estimated to have around one thousand soldiers.

To enhance redundancy of its submarine cables, Taiwan has recently laid Pacific Light Cable Network connecting Taiwan to the US and is building the Apricot cable system that will link Taiwan to Japan and other regional neighbours. Taiwan's backup satellite communications network will provide additional redundancy to undersea cables. ICEF cyber operations are being developed to assess the planning capabilities of the People's Liberation Army, disrupt logistical systems, and access information to gain insight into Beijing's objectives.[16]

US Cyber Command conducts full spectrum cyber operations

On December 19, it was revealed by Gen. Paul Nakasone, who heads both the National Security Agency and the US Cyber Command (CYBERCOM), that a "full spectrum" cyber operation was launched to protect election systems and other critical systems from foreign actors.

The CYBERCOM was given powers by the National Security Presidential Memoranda 13, and the National Defense Authorization Act (NDAA) that cleared the way for clandestine digital operations.[17] The Command, armed with intelligence from the NSA, deployed "hunt forward" teams in Eastern Europe, and launched a digital strike against the Russian Internet Research Agency during the mid-term election. The command also acted against Iranian

[16] Taiwan's Offensive Cyber Capabilities and Ramifications for a Taiwan-China Conflict | Council on Foreign Relations (cfr.org)

[17] https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

hackers backed by the Islamic Revolutionary Guard Corps in the run-up to the 2020 presidential election.[18]

The Cyber National Mission Force (CNMF), which serves as CYBERCOM's lead organization on election security, is composed of 39 joint cyber teams with over 2,000 military and civilian personnel. It also trains Ukraine cyber personnel against Russian hackers and battles against cyber espionage and ransomware.[19]

US Agencies Issue Guidance on Threats to 5G Network Slicing

On December 15, the US National Security Agency (NSA) along with other cyber security agencies have released a guidance on the security risks associated with 5G network slicing and mitigation strategies, which may be useful for Indian stakeholders.

Network slicing, that provides different logical networks on a single physical network, enables data and security isolation. However, lack of proper isolation may lead to threats to the confidentiality, integrity, and availability, leading to denial of service (DoS), Man-in-the-Middle (MitM) attacks, and configuration attacks, on the 5G network. The Guidelines have suggested several mitigation techniques including Zero Trust Architecture (ZTA), Multi-Layer Security (MLS), Post-Quantum Cryptography (PQC), and Isolation.[20]

The US accelerates efforts to retain technology leadership

The US has accelerated its efforts to 'onshore' and 'friend-shore' manufacturing of semiconductor. On December 6, the US President visited the project site of Taiwan Semiconductor Manufacturing Company's (TSMC) plant in Arizona and called the project a potential "gamechanger" for the US semiconductor supply chain. TSMC is building a chip manufacturing facility, with up to $40 billion, to make 3-nanometer chips.[21] Such advanced chips are vital for smartphones, autonomous vehicles, supercomputers, and AI technologies. By 2026, it is scheduled to supply Apple and chipmakers AMD and Nvidia. About 22 percent of all chips and more than 90 percent of the most advanced chips are currently made in Taiwan.

[18] Cyber Command conducted offensive operations to protect midterm elections - The Record by Recorded Future
[19] Cyber National Mission Force elevated in fight against foreign hackers - The Record by Recorded Future
[20] ESF Potential Threats to 5G Network Slicing (defense.gov)
[21] (Nanometre size refers to the distance between transistors on a chip)

In July, the US lawmakers passed the $52.7 billion CHIPS and Science Act package to boost the domestic semiconductor industry. The US is also trying to collaborate with regional alliances including Quad countries, in a complex balancing act that has implications for global technological leadership and geopolitics.[22]

Along with these incentive measures, the US continues to impose curbs China's access to American technologies and components. On December 15, the U.S. Commerce Department expanded the Entity List, that identified Chinese chipmaker Yangtze Memory Technologies Company (YMTC) along with other 36 Chinese companies and research organization, in an export controls blacklist, citing concerns over national security, US interests and human rights. This move has further escalated tension over technology competition between the two countries.[23]

According to a RAND Corporation report, the export controls won't affect the Chinese military, as they rely on older, less sophisticated chips.[24]

EU Commission drafts cross border data privacy framework

On December 13, the European Commission launched the draft 'adequacy decision' for the EU-US Data Privacy Framework, that address the concerns raised by the Court of Justice of the European Union in July 2020. The EU's Court had invalidated the earlier data protection framework for trans-Atlantic data flows- "Privacy Shield", on the premise that the US government could still snoop on transferred EU data under Section 702 of the Foreign Intelligence Surveillance Act.[25]

The US regulations were changed following an agreement between the EU and the US in March 2022.[26] The draft adequacy decision, assesses the US legal framework and concludes that it provides comparable safeguards to data transferred from the EU. It has now been published and transmitted to the European Data Protection Board (EDPB) for its opinion.[27] This draft could be a reference for consideration in the Indian draft Digital Personal Data Protection Bill 2022.

[22] U.S. should brace for '10-year' chip curbs against China: analyst - Nikkei Asia
[23] U.S. blacklists China chipmaker YMTC, AI champion Cambricon, others - Nikkei Asia
[24] Securing the Microelectronics Supply Chain_ Four Policy Issues for the U.S. Department of Defense to Consider.pdf
[25] The Foreign Intelligence Surveillance Act of 1978 (FISA) | Bureau of Justice Assistance (ojp.gov)
[26] Joint Statement on Trans-Atlantic Data Privacy Framework (europa.eu)
[27] Commission publishes draft adequacy decision for the EU-US (europa.eu)

International Cooperation

India conducts counter terrorism exercise with SCO members

On December 14-15, the Indian National Security Council Secretariat (NSCS), conducted a practical seminar on "Securing the Cyberspace Frontiers", with SCO's Regional Anti-Terrorists Structure (RATS), with a special focus on examining and deliberating on issues related to misuse of internet by Terrorists, Separatists and Extremists (TS&E). SCO RATS seminar participants included members from Kazakhstan, China, Kyrgyzstan, Pakistan, Russia, Tajikistan, Uzbekistan, and India. The participants discussed the challenges posed by the terrorists in misusing social media and employing it as "tool kit" besides the use of emerging technologies including Dark Web, and cryptocurrencies.[28]

***

[28] RATS SCO Practical Seminar on "SECURING THE CYBER SPACE FRONTIERS" Organized by National Security Council Secretariat of India (pib.gov.in)

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

www.delhipolicygroup.org