Delhi Policy Group

Advancing India's Rise as a Leading Power

DPG CYBER REVIEW

APRIL 2022

Volume III, Issue 4 | April 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 4
April 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 4
April 2022

Contents

Abstract

A cyber-attack on the public sector oil major Oil India Limited (OIL) disrupted its IT system and was accompanied by a ransom demand of USD 7.5 million. Chinese hackers targeted India's northern power grid along the disputed India-China border in Ladakh.

To enhance cyber preparedness and resilience against such attacks, the National Security Council Secretariat conducted its maiden 10-day National Cyber Exercise (NCX), at which around 150 senior management and technical personnel of Government/Critical Sector organisations and security agencies were trained on contemporary cyber threats, and the handling of cyber incidents, and response.

Prime Minister Modi urged industry to make India a semiconductor hub of the world based on the principles of high technology, high quality and high reliability. In response to an incentive package of $10-billion towards capability development in the semiconductor field, five proposals have been received to set up electronic chip and display manufacturing plants with investment of $20.5 billion (₹1.53 lakh crore).

The much-awaited recommendations of the Telecom Regulatory Authority of India (TRAI) on 5G spectrums were released on April 28, paving the way for spectrum sale and expected 5G rollouts by August 15, India's Independence Day.

CERT-In issued directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents under the provisions of Information Technology Act, 2000, requiring organizations to report cybersecurity incidents to CERT-IN within six hours.

NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) conducted the thirteenth edition of Locked Shields, its annual live-fire cyber defense exercise, from April 19 to April 22. More than 2,000 participants from over 32 countries tested the readiness of national, military, and civilian IT systems against attacks targeting vital services and critical infrastructure by simulating a realistic, large-scale assault against an entire nation.

The European Union reached agreement to enact a 'Digital Services Law requiring companies to more aggressively police their platforms for illicit content or risk billions of dollars in fines.

Elon Musk launched a successful bid for the social media company Twitter, with a $44 billion deal to take it private. He appears likely to strengthen the company's position on free speech.

The fourth India-U.S. 2+2 Ministerial Dialogue endorsed the 2021 reports of the UN Open Ended Working Group (OEWG) and the UN Group of Governmental Experts (UNGGE), which articulate a framework of responsible state behavior in cyberspace, and committed to work together in future multilateral negotiations to encourage States to implement the framework.

India and the EU agreed to launch a Trade and Technology Council. This strategic coordination mechanism will allow both partners to tackle challenges at the nexus of trade, trusted technology and security.

National Developments

Cyber-attacks affect India's oil and power sectors

On April 10, public sector oil company, Oil India Limited (OIL), suffered a cyberattack disrupting its operations in Assam. The cyber-attack on workstations of OIL's Geological and Reservoir department disrupted its IT system and was accompanied by a ransom demand of USD 7.5 million (over Rs 57 crore). The impact was limited because the attack came on a Sunday when only a handful of workstations were in use. Security agencies are probing the attack for the possible role of cyber- criminal syndicates or foreign-backed players.[1]The company has since secured its data and disabled the impacted systems. A private cyber security agency has also been engaged to assist with remedial actions.[2]

On April 6, the threat intelligence firm 'Recorded Future' reported that Chinese hackers targeted India's power grid to collect intelligence from its North Indian centres. The hackers focused on at least seven "load dispatch" centres in northern India that are responsible for carrying out real-time operations for grid control and electricity dispersal in areas near the disputed India-China border in Ladakh.

China's foreign affairs ministry spokesman denied allegations that the Chinese government was behind the attack.

India conducts its maiden National Cyber Exercise

To beef up cyber preparedness in wake of these cyber-attacks on Oil India and other critical information infrastructure, the National Security Council Secretariat conducted its maiden 10-day National Cyber Exercise (NCX India) from April 18-29 to train senior management and technical personnel of Government/Critical Sector organisations and agencies on contemporary cyber threats, the handling of cyber incidents, and response. Around 150 government officials, including Chief Information Security Officers (CISOs) from critical information infrastructure attended the closed-door event.

[1] IB, Central cyber security agencies to probe ransomware attack on Oil India, IT Security News, ET CISO (indiatimes.com)
[2] Oil India suffers cyber attack, receives Rs 57 crore ransom demand | Business Standard News (business-standard.com)

The NCSC highlighted the need for a strong cyber defence posture and deterrence to meet the challenges of "quasi-kinetic" modern conflicts as illustrated in the Russia-Ukraine War.[3]

Push to make India a Semiconductor hub

While operational readiness to defend sovereign cyber space is a must, India needs to also develop inner strength and capabilities through indigenous production of strategic assets, including semiconductor chips. The country has an exceptional semiconductor design talent pool, with 20% of the world's chip design engineers. India's consumption of semiconductors is expected to cross $80 billion by 2026 and $110 billion by 2030.

On April 29, Prime Minister Modi urged industry to make India a semiconductor hub of the world based on the principles of high technology, high quality and high reliability. The government has put in place a supportive policy environment towards this end, with attractive incentives as part of India Semiconductor Mission.

In response to the $10-billion package as incentive towards capability development in the semiconductor field, the government has received applications for design and compound semiconductors while five companies have proposed electronic chip and display manufacturing plants with investment of $20.5 billion (₹1.53 lakh crore). The pre-evaluation has progressed well and the final evaluation will be completed within six to eight months. The IT Ministry is also engaging with larger companies like Intel, TSMC and Samsung, for setting up semiconductor plants within a timeframe of 2-3 years.[4] Indian states have also jumped into the fray by offering incentives such as capital subsidy of 25% on land, waiver of electricity duty, and additional subsidy on plant and machinery to attract chipmakers.

5G roll out amid spectrum controversies

The much-awaited recommendations of the Telecom Regulatory Authority of India (TRAI) on 5G spectrums were released on April 28, paving the way for spectrum sale and likely 5G rollouts by August 15, India's Independence Day. The recommendation clears auction of more than 100,000 MHz of airwaves by June. The regulator has called for rationalisation of spectrum caps in the

[3] https://www.theweek.in/news/india/2022/04/18/doval-points-to-ukraine-russia-conflict-to-show-risk-of-cyber-war.html

[4] semiconductor manufacturing: Govt to finalise chipmakers under incentive scheme in 6-8 months: Vaishnaw, Telecom News, ET Telecom (indiatimes.com)

runup to the 5G airwaves sale. It has proposed a 40% cap on combined spectrum holding in sub-1 GHz bands, and a 40% cap on combined airwave holdings in the 1800 MHz, 2100 MHz, 2300 MHz and 2500 MHz bands. It has recommended an individual band-specific cap of 40% for 5G bands such as 3.3-3.67 GHz and the mmWave bands.

TRAI has also set rates for new bands in the 600 MHz and millimetre wave (mmWave) and proposed that such spectrum be assigned in a contiguous manner. It has, however, decided against auctioning airwaves in the 526-612 MHz range as these are being used by the ministry of information and broadcasting (MIB).

On April 29, the Digital Communications Commission (DCC), DoT's highest decision-making body, termed the pricing recommendations for 5G spectrum as reasonable but decided not to allot spectrum directly to corporate entities for private 5G networks, contrary to TRAI recommendations. Instead, it suggested that they partner with licensed telecom Service providers (TSP). The technology companies fear such a move would cause a huge setback to India's broader ambitions of digitalising its industry and leveraging its current geopolitical advantage. A final call will be taken by the Union Cabinet.[5]

The DCC also decided that airwaves in the millimetre wave band of 27.5 GHz to 28.5 GHz band – which was sought by satellite companies for broadband-from-space services – should be kept out of the 5G spectrum auction. TRAI had suggested that telecom and satcom service providers use the band on a "coexistence basis".[6]

Review and strengthening of IT Act

The need for an overall framework of laws, rules and policies to strengthen Indian Cyber Space has been widely recognised. In a first step towards overhauling of the two-decade old IT Act, a new legislative framework is being proposed for public consultation in May 2022.

As part of the process, the Indian government has issued new directives requiring organizations to report cybersecurity incidents to CERT-IN within six hours, even if those incidents are port or vulnerability scans of computer systems. On April 28, CERT-In issued directions relating to information security practices, procedure, prevention, response and reporting of cyber

[5] Telecom Regulatory Authority of India: Top DoT body accepts Trai's 5G base price suggestions, Telecom News, ET Telecom (indiatimes.com)
[6] Satcom firms urge DoT not to offer 28 GHz spectrum band for 5G services, Telecom News, ET Telecom (indiatimes.com)

incidents under the provisions of sub-section (6) of section 70B of the Information Technology Act, 2000. These directions will become effective after 60 days and will enhance overall cyber security posture to ensure safe and trusted Internet in the country.[7]

[7] Cert-In - Home Page

International Developments

New Bureau in State Department

Amid warnings of heightened risks of Russian cyberattacks on U.S. critical infrastructure and other sectors, the US State Department has launched its new 'Bureau of Cyberspace and Digital Policy' on April 4, aimed at emerging technology issues in diplomacy. The Bureau will focus on the distribution of cyber aid to foreign nations, international standard setting in bodies such as the International Telecommunication Union, and the promotion of digital rights and freedoms. It will address ransomware, cyberspace regulation, and alternatives to Chinese 5G technology.[8]

Iran Foiled Cyberattacks on Public Services

On April 24, Iran reportedly thwarted massive cyberattacks that sought to target the infrastructure of more than 100 public sector agencies and public services, both government and privately owned. Reports indicated that unidentified parties behind the cyberattacks used Internet Protocols in the Netherlands, Britain and the United States to stage the attacks.

Internet Outages in French Cities after Cable 'Attacks'

On April 27, Internet and phone services in several French cities were affected after fibre optic cables were cut overnight in suspected attacks on critical data infrastructure. Problems were reported by users across the country. The cuts targeted so-called "backbone" cables which carry huge quantities of data between different regions and typically run along motorways or rail tracks. The Paris-Lyon and Paris-Strasbourg links were majorly targeted.[9]

NATO conducts Locked Shields cyber defense exercise

NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) conducted the thirteenth edition of Locked Shields, its annual live-fire cyber defense exercise, from April 19-22 April. More than 2,000 participants from over 32 countries tested the readiness of national, military and civilian IT systems against attacks targeting vital services and critical infrastructure by simulating a realistic, large-scale assault against an entire nation. The exercise included the simulation of a reserve management and financial messaging system of a central bank. A 5G standalone mobile communication platform was deployed

[8] State Department formally launches new cyber bureau | The Hill
[9] Internet Outages in French Cities After Cable 'Attacks': Operator | SecurityWeek.Com

as part of a critical infrastructure to give a first experience to cyber defenders about upcoming technology change.

EU Digital Services Act

On April 22, the European Union reached agreement to pass a 'Digital Services Act' which is intended to address social media's societal harm by requiring companies to aggressively police their platforms for illicit content or risk billions of dollars in fines. The legislation would force large technology companies and other internet services to combat misinformation, disclose how their services amplify divisive content and stop targeting online ads based on a person's ethnicity, religion or sexual orientation. The law aims to end an era of self-regulation by tech companies and addresses online speech, unlike in the United States because of First Amendment protections.[10]

In March, the 27-nation bloc had agreed to adopt a 'Digital Markets Act', to counter anticompetitive behaviour by big technology companies. The legislation aims to prevent dangerous disinformation from going viral and avoid unsafe products being offered on marketplaces.[11]

The EU intends to open an office in San Francisco, to support communication with tech-companies related to the Digital Services Act (DSA) and the Digital Markers Act (DMA).[12]

Elon Musk takes over Twitter with a new vision

On April 25, the Twitter board accepted Elon Musk's offer to buy the social media company in a $44 billion to take it private. Musk has said that he wants to strengthen Twitter's position on "free speech," to make Twitter the "de facto public town square", and to promote global democracy. Musk's vision may end the biases that favour only one kind of narrative and the existing trend for Twitter to arbitrarily delete content or de-platform prompted by big tech's business interests.[13]

The deal has also triggered optimism in some quarters that the mission to "authenticate all humans" and defeat spam bots on Twitter could spur

[10] https://www.nytimes.com/2022/04/22/technology/european-union-social-media-law.html
[11] E.U. Takes Aim at Big Tech's Power With Landmark Digital Act - The New York Times (nytimes.com)
[12] https://www.politico.eu/article/as-big-tech-crackdown-looms-eu-to-open-silicon-valley-base/
[13] https://www.wsj.com/articles/elon-musk-rebrands-twitter-partisan-democrats-hunter-laptop-donald-trump-ban-censor-social-media-free-speech-11651265590

cybersecurity tech innovation around identity, multi-factor authentication and botnet detection. Industry watchers are said to be closer attention to Musk's larger goals around security technology innovation.[14]

On April 26, it was clarified that the Indian government's expectations of accountability, safety and trust of all intermediaries operating in India including Twitter, remain unchanged irrespective of the Musk takeover and his new vision.[15]

[14] Twitter accepts Elon Musk's buyout deal (cnbc.com)
[15] rajeev chandrasekhar: Govt's expectations of accountability remain unchanged: Chandrasekhar on Elon Musk-Twitter deal - The Economic Times (indiatimes.com)

International Cooperation

Joint Statement of Fourth India-U.S. 2+2 Ministerial Dialogue

The fourth India-U.S. 2+2 Ministerial Dialogue was held on April 11. The Joint Statement at the end of the Dialogue covered the following important issues pertaining to cooperation in cyber space and digital technologies.

Considering growing national security threats from both state and non-state malicious cyber actors, the Ministers recognized the importance of an open, interoperable, secure, and reliable Internet and stable cyberspace. Both sides reaffirmed the 2021 reports of the UN Open Ended Working Group (OEWG) and the UN Group of Governmental Experts (UNGGE), which articulate a framework of responsible state behaviour in cyberspace and committed to work together in future multilateral negotiations to encourage States to implement the framework. They confirmed their intent to work closely as part of ongoing efforts to counter the use of information communications technologies for criminal purposes.

The Ministers appreciated the recent and upcoming meetings of the India-U.S. Cyber Dialogue and the Information and Communication Technology (ICT) Working Group to deepen cybersecurity cooperation. They strongly condemned ransomware and other cyber-related crimes and recognised the need to bolster protection of critical networks and infrastructure.

Reflecting on the positive science and technology cooperation between the two countries, the Ministers welcomed the announcement of a Joint Commission Meeting on Science and Technology in 2022, to discuss future science and technology collaboration."[16]

India and the EU launch a Trade and Technology Council

India and the EU agreed to launch a Trade and Technology Council at a meeting of the Prime Minister of India and President of the European Commission on April 25. This strategic coordination mechanism will allow both partners to tackle challenges at the nexus of trade, trusted technology and security, and thus deepen cooperation in these fields between the EU and India. Both sides agreed that rapid changes in the geopolitical environment highlight the need for joint in-depth strategic engagement. The Trade and Technology Council will provide the political steer and the necessary structure to operationalise political decisions, coordinate technical work, and report to the

[16] Joint Statement on the Fourth India-U.S. 2+2 Ministerial Dialogue (mea.gov.in)

political level to ensure implementation and follow-up in areas that are important for the sustainable progress of the Indian and European economies. The decision to set up a Trade and Technology Council will be a first for India with any of its partners and is the second for the EU following one with the US.[17]

60 countries join hands for open, free and secure global internet

The White House announced on April 28 that the US, the UK, all the European Union (EU) member states and 32 non-EU countries have signed a "Declaration for the Future of the Internet" that calls for an "open, free, global, interoperable, reliable, and secure" internet. India, China, and Russia are notable exclusions.

The Declaration pledged that the Internet should function as a single, decentralised network of networks with global reach, governed by a multistakeholder approach, in which governments and relevant authorities collaborate with academics, civil society, the private sector, the technical community, and others. It reaffirms and recommits its partners to a single global Internet that "fosters competition, privacy, and respect for human rights as reflected in the Universal Declaration of Human Rights".[18]

***

[17] India-EU: Joint Press Release on Launching the Trade and Technology Council (mea.gov.in)

[18] https://www.news18.com/news/tech/india-china-russia-missing-from-future-of-the-internet-pledge-inked-by-us-eu-uk-and-32-other-nations-5078995.html

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

www.delhipolicygroup.org