MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

# CYBER *Digest*

**July 2023**

- Takeaways from Prime Minister Narendra Modi's visit to the US
- Reports on India's CoWIN data breach
- US Cybercom 'hunt forward" teams in Latin America
- Crackdown on Iranian Opposition operated hacker centers in Albania
- The EU to ban Chinese suppliers from internal networks
- Vulnerability in MOVEit software exploited by cybercriminals
- Report highlights North Korean social engineering tactics
- Ransomware attack on Argentinian Securities Commission
- India File

## Takeaways from Prime Minister Narendra Modi's visit to the US

The joint statement issued at the end of Prime Minister Modi's state visit to the United States emphasised broadening the India-US partnership in critical areas of technologies, such as developing trusted and secure 5G and 6G telecom networks, cooperation on Artificial Intelligence (AI) and semiconductors.[1] Joint cooperation on high-performance computing and space is also on the tech cooperation agenda. The joint declaration also affirmed collaboration on human spaceflight, including sending an Indian astronaut to the International Space Station in 2024 oppression.

American companies such as Micron, Google, and Applied Materials have announced big investments in India.[2] Chipmaker Micron Technology has pledged to build an assembly and test facility in India. On the other hand, Applied Materials will create a campus where the staff will work alongside leading global and domestic suppliers, and top research and academic institutions to develop a new chipmaking kit. The declaration also affirmed that the Initiative for Critical and Emerging Technologies (iCET) has emerged as an important framework for technical cooperation between both the nations. The iCET was announced by India and the US in May 2022, which was seen as a significant step towards elevating and expanding strategic technology partnership and defense industrial cooperation between the governments, businesses, and academic institutions of both countries.[3]

## Reports on India's CoWIN data breach

According to Indian media reports, India's COVID-19 vaccine booking portal, CoWIN, was compromised, and the sensitive personal information of thousands of users was leaked on the Telegram social messaging app.[4] The reports claimed that a Telegram bot was revealing users' sensitive data when inquired about an individual's phone number. The leaked information consisted of the name, Aadhaar number, PAN number, passport number, date of birth, location, gender, and the institute from where they got vaccinated. However, the government, in its response has denied any such breach and clarified that reports are without any basis and mischievous in nature.[5] The government also reiterated that the data of vaccinated beneficiaries could not be shared with any bot without OTP. The development team of the CoWIN also confirmed that there are no public application programming interfaces (APIs) where data can be pulled without OTP. Furthermore, the Indian Computer Emergency Response Team (CERT-In), in its initial investigation, has pointed out that the backend database for the Telegram bot was not directly accessing the APIs of the CoWIN database.

## US Cybercom 'hunt forward" teams in Latin America

According to reports, as part of the 'hunt forward' operation, the US Cyber Command deployed a team of operators to a South American nation.[6] These operations involve sending defensively oriented cyber protection teams from the US military

Cyber National Mission Force (CNMF) to foreign nations at their invitation to look for malicious activity on their networks. Given that these hunt-forward operations are conducted at the invitation of host nations, public disclosure of details is highly sensitive, and the host government's permission is required.

## Crackdown on Iranian Opposition operated hacker centers in Albania

Albanian authorities raided a camp for members of the exiled Iranian opposition group Mujahedeen-e-Khalq (MEK) to seize computer devices allegedly used for cyber-attacks against foreign institutions.[7] There have been instances when MEK members have accepted running hacking operations against the Iranian government and institutions. The raid is believed to be undertaken in response to the violation of the agreement between the Albanian government and MEK that forbade political activity by the exiled group in Albania. In May 2023, the hacktivist group affiliated with MEK hacked into the Islamic Republic's foreign ministry servers, disabling 210 sites and online services while leaking a large batch of documents.[8]

## The EU to ban Chinese suppliers from internal networks

Recognizing the significance of securing 5G networks to safeguard critical infrastructures such as energy, transport, health, and finance, the EU has announced moves to block the Chinese firms Huawei and ZTE from EU research funding and stop contracting operators using Chinese equipments.[9] According to the statement, Chinese suppliers Huawei and ZTE pose higher risks than other 5G suppliers. EU countries are preparing legislative measures to allow security services to block contracts with these suppliers.

## Vulnerability in MOVEit software exploited by cybercriminals

It was reported that criminals had exploited a vulnerability in Progress Software's MOVEit file transfer app, which thousands of organizations use worldwide.[10] Due to this, a number of organizations whose supply chains use the app have suffered a data breach, with customer and employee data being stolen. According to Progress, the company reported a vulnerability in MOVEit Transfer and MOVEit Cloud and, upon discovery of the breach, took immediate action to release a security patch.[11] However, the number of victims of the security flaw has grown by millions, including the biggest US pension fund, Calpers. Siemens Energy has also confirmed the data theft during the Clop ransomware attacks using a zero-day vulnerability in the MOVEit Transfer platform.[12]

## Report highlights North Korean social engineering tactics

The US Department of State, the Federal Bureau of Investigation, the National Security Agency, and partners from the Republic of Korea Ministry of Foreign Affairs, the National Police Agency, and the National Intelligence Service released a cybersecurity advisory.[13] The document highlighted the social engineering and hacking threat posed by the North Korean cyber group known as Kimsuky. The group is known for conducting large-scale social engineering campaigns in which the victims are manipulated and compromised for the purpose of intelligence gathering. The advisory also provided a broader overview of North Korea's cyber program, providing the regime with broad intelligence collection and espionage capabilities.

## Ransomware attack on Argentinian Securities Commission

The Argentinian government announced that its National Securities Commission (CNV) suffered a massive ransomware attack orchestrated by the hacking group Medusa.[14] According to reports, the group was able to access systems hosting thousands of documents and databases hosted on the agency's computers. The hackers demanded payment of US$500,000 and threatened to release 1.5 terabytes of financial information to the public within a week if the demands were not met. The Medusa ransomware operation first emerged in June 2021, which later swiftly expanded to target corporate victims for the ransom.

## India File

- The Standing Committee of Finance in the Indian Parliament deliberated on the issue of cybersecurity and rising incidents of cyber/white-collar crimes as lawmakers quizzed experts from the industry about various facets of unlawful activities in cyberspace.[15] The issue of fraud lending apps also came up for discussion at the meeting. Senior officials of different fintech firms and public policy and advocacy groups were among the industry stakeholders who deposed before the committee.
- All India Institute of Medical Sciences (AIIMS) New Delhi reportedly thwarted a malware attack on its servers, ensuring services remain fully secure and functional.[16] This is the second cyber incident against AIIMS within a year, as the institution faced disruption in services due to a cyberattack in November 2022. The institute confirmed the attack on its official Twitter account and assured that deployed cybersecurity systems neutralized the threat.
- According to an assessment, India is expected to face a shortage of around 3 million cybersecurity professionals by the end of 2023.[17] The shortage poses a severe challenge to organizations in effectively managing their cybersecurity posture and responding the emerging threats, given the proliferation of connected devices and the Internet of Things (IoT).
- The third G20 Digital Economy Working Group (DEWG) meeting was organized in Pune with agendas including the Global DPI (digital public infrastructure) Summit and Global DPI Exhibition.[18] The summit provided a global platform to discuss issues, including- an 'overview of digital public infrastructure,' 'digital identities for empowering people,' ''digital payments and financial inclusion' etc.
- India's cybersecurity watchdog Indian Computer Emergency Response Team

(CERT-In), has issued guidelines on information security practices to be followed by government entities and industries to keep them protected from online threats.[19] The guidelines include various security domains such as network security, identity and access management, application security, data security, third-party outsourcing, hardening procedures, security monitoring, incident management, and security auditing.

- The 'ARF Workshop on Fostering Professionals in the field of Security of and in the use of ICTs' was held on 13.6.2023 in Hanoi, Vietnam with Shri Ravi Shanker Goel, Director (CD) in attendance. The second ARF Workshop on "Terminology in the field of Security of and in the use of ICTs in the context of Confidence Building" was also held on 21.6.2023, but in virtual mode.

[1] The Times of India, India-US joint statement hails giant leap in technology partnership and opportunities, 23 June 2023, https://timesofindia.indiatimes.com/business/india-business/india-us-joint-statement-hails-giant-leap-in-technology-partnership-and-opportunities/articleshow/101224577.cms

[2] The Register, Micron, Applied Materials make big investments in India, 23 June 2023, https://www.theregister.com/2023/06/23/micron_india_assembly_facility/

[3] The White House, FACT SHEET: United States and India Elevate Strategic Partnership with the initiative on Critical and Emerging Technology (iCET), 31 January 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/01/31/fact-sheet-united-states-and-india-elevate-strategic-partnership-with-the-initiative-on-critical-and-emerging-technology-icet/

[4] WION, Explained: CoWIN data leak, and how bots stoke privacy tensions, 13 June 2023, https://www.wionews.com/industry/explained-cowin-data-leak-and-how-bots-stoke-privacy-tensions-603858

[55] PIB, Co-WIN portal of Health Ministry is Completely Safe with safeguards for Data Privacy, 12 June 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1931691

[6] Defencescoop, US Cyber Command conducts 'hunt forward' mission in Latin America for first time, official says, 8 June 2023, https://defensescoop.com/2023/06/08/us-cyber-command-conducts-hunt-forward-mission-in-latin-america-for-first-time-official-says/

[7] AP News, Police raid Iranian opposition camp in Albania, seize computers, 21 June 2023, https://apnews.com/article/albania-mek-iranian-opposition-police-raid-851dcb5fc32cd6bc60206e342eea7b16

[8] Iran International, Hacktivists Target Iran's Foreign Ministry, Leak Trove Of Data, 7 May 2023, https://www.iranintl.com/en/202305079860

[9] Politico, EU executive to block Huawei from its contracts, 15 June 2023, https://www.politico.eu/article/huawei-commission-eu-executive-to-block-from-its-contracts/

[10] National Cyber Security Centre, MOVEit vulnerability and data extortion incident, 27 June 2023, https://www.ncsc.gov.uk/information/moveit-vulnerability

[11] Progress, MOVEit Transfer and MOVEit Cloud Vulnerability, 27 June 2023, https://www.progress.com/security/moveit-transfer-and-moveit-cloud-vulnerability

[12] Bleeping Computer, Siemens Energy confirms data breach after MOVEit data-theft attack, 27 June 2023, https://www.bleepingcomputer.com/news/security/siemens-energy-confirms-data-breach-after-moveit-data-theft-attack/

[13] US Department of State, U.S. and ROK Agencies Cybersecurity Alert: The Democratic People's Republic of Korea (DPRK) Social Engineering Campaigns Targeting Think Tanks, Academia, and News Media, 1 June 2023, https://www.state.gov/u-s-and-rok-agencies-cybersecurity-alert-the-democratic-peoples-republic-of-korea-dprk-social-engineering-campaigns-targeting-think-tanks-academia-and-news-media/

[14] Buenos Aires Herald, Massive ransomware attack hits National Securities Commission, 12 June 2023, https://buenosairesherald.com/business/tech/massive-ransomware-attack-hits-national-securities-commission

[15] The Economic Times, Parliamentary panel on finance debates cyber security, rising white collar crimes, 4 June 2023, https://economictimes.indiatimes.com/tech/technology/parliamentary-panel-on-finance-debates-cyber-security-rising-white-collar-crimes/articleshow/100741974.cms?from=mdr

[16] The Telegraph, AIIMS Delhi hit by fresh cyberattack for second time in a year, 6 June 2023, https://www.telegraphindia.com/india/all-india-institute-of-medical-science-delhi-hit-by-fresh-cyberattack-for-second-time-in-a-year/cid/1942831

[17] The Times of India, Challenges faced by cyber security in 2023, 19 June 2023, https://timesofindia.indiatimes.com/blogs/voices/challenges-faced-by-cyber-security-in-2023/

[18] PIB, Third meeting of 'G20 Digital Economy Working Group (DEWG)' concluded on 14 June 2023, 14 June 2023, https://pib.gov.in/PressReleasePage.aspx?PRID=1932370

[19] The Times of India, Cyber security watchdog CERT-In issues guidelines for protection of govt data from cyberattacks, ransomware, 30 June 2023, https://timesofindia.indiatimes.com/india/cyber-security-watchdog-cert-in-issues-guidelines-for-protection-of-govt-data-from-cyberattacks-ransomware/articleshow/101401918.cms?