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

CYBER *Digest*

June 2025

- **Cyberattacks Targeting India Surge Amid Operation Sindoor**
- **Cyberattack Disrupts South African Airways Operations**
- **LockBit Breached, Ransomware Syndicate Turns Victim**
- **North Korean Hackers Cyber Espionage Against Ukraine**
- **Fears Over Chinese Solar Inverters**
- **Japan Passes Active Cyberdefense Law**
- **India File**

Cyberattacks Targeting India Surge Amid Operation Sindoor

During Operation Sindoor, India was hit by a wave of cyberattacks from state-backed actors and hacktivists across multiple countries, targeting critical infrastructure and defense systems.[1] The attacks included DDoS assaults and efforts to steal sensitive data. Notably, 75% of these cyber incidents were directed at government digital infrastructure. Amid rising tensions between India and Pakistan, Maharashtra Cyber identified seven Advanced Persistent Threat (APT) groups behind over 1.5 million cyberattacks on Indian websites following the Pahalgam terror attack.[2] Officials reported that only 150 attacks succeeded, less than 1% of the total, highlighting the effectiveness of India's cyber defenses.

According to an assessment, between April 22 and May 8, 2025, over 200 cyberattacks targeting Indian government and private entities were recorded, primarily by pro-Pakistani and Bangladeshi hacktivist groups.[3] More than 55% of these were Distributed Denial of Service (DDoS) attacks aimed at disrupting server operations. Other tactics included website defacements, data breaches, and information leaks. Social media was flooded with a surge of misinformation campaigns, which the Indian government countered in real time.[4] Despite a mutual understanding between India and Pakistan to cease military hostilities, Indian government websites faced a barrage of cyberattacks originating from Pakistan, Bangladesh, and parts of the Middle East.[5]

As a countermeasure, India's leading stock exchanges, the National Stock Exchange (NSE) and the Bombay Stock Exchange (BSE), temporarily restricted website access from foreign IP addresses following a spike in cyberattacks on critical financial infrastructure.[6]The decision comes after attempted intrusions into one of the exchange's web systems and amid growing concerns over rising cyber threats targeting Indian institutions.

Cyberattack Disrupts South African Airways Operations

South African Airways (SAA) reported that a cyberattack briefly disrupted its website, mobile app, and several internal systems.[7] The airline said its IT team quickly contained the incident, minimizing impact on core flight operations. Customer service channels, including contact centers and sales offices, remained functional throughout. Officials also confirmed that all affected systems were restored the same day. SAA is investigating the root cause and potential data breaches. The incident has been reported to the State Security Agency, the South African Police Service (SAPS), and the Information Regulator. The airline said it would notify anyone whose data may have been compromised.

The attack was claimed by the ransomware gang INC, although SAA has not confirmed the group responsible. INC is known for using double-extortion tactics, demanding ransom for both system decryption and the deletion of stolen data. The group has reportedly carried out multiple attacks, including on airlines like Air Europa (Spain) and Oceanair (US). The transport sector has seen numerous ransomware attacks recently, affecting companies worldwide.[8]

LockBit Breached, Ransomware Syndicate Turns Victim

The ransom-seeking cybercriminal group LockBit appears to have been breached, with leaked data reportedly including chat logs between the hackers and their victims. While the group has not confirmed the breach, analysts who reviewed the material say it appears to be authentic.[9] The group's dark web affiliate panels were defaced and replaced with a message linking to a MySQL database dump. All admin interfaces now show the message: "Don't do crime. CRIME IS BAD xoxo from Prague."[10] It remains unclear who carried out the breach or how it was executed, but the defacement message matches that used in a recent attack on Everest ransomware's dark web site, hinting at a possible connection.

North Korean Hackers Cyber Espionage Against Ukraine

North Korean state-backed hackers have launched a new espionage campaign targeting Ukrainian government entities, likely to gather intelligence related to Russia's war efforts, researchers say.[11] The group, known as TA406, is notorious for spear-phishing campaigns against governments, think tanks, research institutions, and media organizations, particularly in Europe, Japan, Russia, South Korea, and the U.S. Previously focused on Russian targets, TA406 now appears to be shifting its attention to Ukraine. With North Korean troops deployed to support Russian forces since late 2024, the operation is likely aimed at assessing risks to its personnel and determining whether further military aid to Moscow is necessary.

Fears Over Chinese Solar Inverters

According to reports, U.S. energy officials are re-evaluating the security risks of Chinese-made devices critical to renewable energy systems after discovering rogue communication components in some of them.[12] Chinese-made power inverters, widely used to link solar panels, wind turbines, batteries, heat pumps, and EV chargers to power grids, are designed for remote access, with firewalls typically in place to block unauthorized communication. However, U.S. experts have found undocumented communication devices, such as cellular radios, embedded in some Chinese inverters and batteries. These rogue components, not listed in official documentation, could enable hidden communication channels that bypass firewalls, posing serious security threats. The exact number of devices inspected remains unclear.

Japan Passes Active Cyberdefense Law

Japan's Parliament has passed a bill enabling the government to take proactive measures to prevent major cyberattacks.[13] The Upper House approved the active cyber defense legislation with support from both the ruling coalition and the opposition Constitutional Democratic Party. A key provision, respecting the secrecy of communications, was added during Lower House deliberations. The law, set to take full effect in 2027, aligns with Japan's 2022 National Security Strategy, which aims to match or exceed the cyberdefense capabilities of major Western nations.

Under the new framework, the government will monitor and analyze international

communications involving Japan, even during peacetime. If signs of a cyberattack emerge, police and the Self-Defense Forces will be authorized to take countermeasures. Joint police–SDF bases will be established, and public-private cooperation will be promoted through sensitive information sharing. Infrastructure operators will also be required to report cyberattacks.

India File

- A major cyberattack took down the official website of Uttar Haryana Bijli Vitran Nigam Limited (UHBVNL), disrupting key online services, including new electricity connections, and impacting over 50,000 consumers.[14] Senior officials confirmed the breach, stating that a wide range of consumer services had been affected. Cybersecurity teams were working around the clock to contain the damage and restore normal operations.

- In a major midnight crackdown in Andhra Pradesh's Anakapalli, over 100 suspects—including women, were detained for running organized cyber fraud operations across six buildings.[15] Most arrested individuals hailed from northern and northeastern states. Police moved them to a secret location for questioning about their activities, recruitment, and operations. Reports say they targeted victims in the USA, UK, Australia, and other countries. A police official likened the operation to smaller-scale cybercrime hubs seen in Cambodia and Myanmar.

- In a major cyber fraud incident, scammers stole Rs. 11.55 crore from the Himachal Pradesh State Co-operative Bank by hacking into a customer's account.[16] Police reported that the attackers tricked the victim into downloading a malicious mobile app called HimPaisa, which granted them remote access to the device. This access allowed them to breach the bank's internet banking system. The hackers then executed unauthorised transactions, transferring the stolen money to 20 different accounts via NEFT and RTGS channels.

- According to a report, National Cyber Security Co-ordinator Lt. Gen M.U. Nair has completed his tenure after two years.[17] Dr. Narendra Nath Gangavarapu, Joint Secretary at the National Security Council Secretariat, has been appointed interim National Cybersecurity Coordinator. During his time in office, Gen. Nair focused on strengthening India's cyber posture through inter-agency collaboration, development of the National Cybersecurity Strategy and engagement with industry and global partners.

- The government has denied the request of CCTV manufacturing companies to extend the deadline requiring manufacturers to submit hardware, software, and source code for testing in government labs. The stringent new security rules, imposed in April 2025, require CCTV cameras to meet strict cybersecurity standards, including tamper-proof enclosures and strong encryption.[18] Then Minister of State for Communications and IT Sanjay Dhotre had informed the Lok Sabha in 2021 that one million cameras in government organisations were from Chinese companies and pose potential security risks as video data could be transferred to servers located abroad.[19]

[1] The Times of India, Operation Sindoor: Govt digital infrastructure faced 75% of cyber attacks, 14 May 2025, https://timesofindia.indiatimes.com/city/hyderabad/operation-sindoor-as-pak-drones-took-to-skies-hackers-attacked-india-via-cloud/articleshow/121146853.cms

[2] WION, Over 1.5 million cyber attacks, but not even 1% successful | Here's how India outsmarted Pakistani hackers, 14 May 2025, https://www.wionews.com/india-news/over-15-mn-cyber-attacks-but-not-even-1-successful-heres-how-india-outsmarted-pakistani-hackers-9065615

[3] The New Indian Express, 500 Indian govt, pvt entities targeted by hacktivist groups, 11 May 2025, https://www.newindianexpress.com/states/kerala/2025/May/11/500-indian-govt-pvt-entities-targeted-by-hacktivist-groups

[4] CNBC TV18, Inside the misinformation Tsunami around India-Pakistan cyber threats, 12 May 2025, https://www.cnbctv18.com/technology/explainer-dance-of-the-hillary-fake-viral-message-india-pakistan-cyber-conflict-19603297.htm

[5] The Economic Times, Cyber attacks on India continue even after understanding with Pak: Cyber officials, 12 May 2025, https://economictimes.indiatimes.com/news/india/cyber-attacks-on-india-continue-even-after-understanding-with-pak-cyber-officials/articleshow/121116147.cms

[6] The 420, NSE, BSE Under Siege? Stock Exchanges Restrict Foreign Web Access Amid Cyberattack Surge, 9 May 2025, https://the420.in/nse-bse-curb-foreign-access-after-cyberattack-surge-2025/

[7] The Record, South African Airways says cyberattack disrupted operational systems, 8 May 2025, https://therecord.media/south-african-airways-cyberattack-disrupted

[8] Comparitech blog, Ransomware gang INC claims recent attack on South African Airways, 16 May 2025, https://www.comparitech.com/news/ransomware-gang-inc-claims-recent-attack-on-south-african-airways/

[9] Reuters, Ransomware group Lockbit appears to have been hacked, analysts say, 12 May 2025, https://www.reuters.com/technology/ransomware-group-lockbit-appears-have-been-hacked-analysts-say-2025-05-08/

[10] Bleeping Computer, LockBit ransomware gang hacked, victim negotiations exposed, 7 May 2025, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-hacked-victim-negotiations-exposed/

[11] The Record, Japan enacts new Active Cyberdefense Law allowing for offensive cyber operations, 16 May 2025, https://therecord.media/japan-enacts-new-law-allowing-offensive-cyber-operations

[12] Reuters, Rogue communication devices found in Chinese solar power inverters, 14 May 2025, https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/

[13] The Japan Times, Japan enacts active cyberdefense law, 16 May 2025, https://www.japantimes.co.jp/news/2025/05/16/japan/politics/cyber-bill-enactment/

[14] The 420, Cyberattack Shuts Down Haryana Power Portal, 50,000+ Consumers Affected, 20 May 2025, https://the420.in/haryana-power-utility-cyberattack-uhbvnl-website-down-electricity-services-hit/

[15] Times of India, Myanmar-like cybercrime compound busted in AP, 22 May 2025, https://timesofindia.indiatimes.com/city/hyderabad/myanmar-like-cybercrime-compound-busted-in-ap/articleshow/121323959.cms

[16] India Today, Rs 11.5 crore stolen in cyber heist at Himachal Co-operative Bank, 20 May 2025, https://www.indiatoday.in/india/story/himachal-pradesh-bank-account-hackers-steal-rs-115-crore-cert-central-agency-probe-2727542-2025-05-20

[17] Bankinfosecurity, India's Top Cyber Coordinator Leaves After Two Years, 3 June 2025, https://www.bankinfosecurity.asia/indias-top-cyber-coordinator-leaves-after-two-years-a-28582

[18] Reuters, India's alarm over Chinese spying rocks the surveillance industry, 28 May 2025, https://www.reuters.com/world/china/indias-alarm-over-chinese-spying-rocks-surveillance-industry-2025-05-28/

[19] Economic Times, Around 10 lakh Chinese CCTV camera installed in govt institutions: Sanjay Dhotre, 17 March 2021, https://economictimes.indiatimes.com/news/politics-and-nation/around-10-lakh-chinese-cctv-camera-installed-in-govt-institutions-sanjay-dhotre/articleshow/81554066.cms