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

CYBER *Digest*

April 2025

- Cyberattack Targets Polish Space Agency, Says Minister
- Cyberattack Hits Russian Telecom Sector, Disruptions Reported
- Massive Outage Hits X, Services Down Worldwide
- Chinese Authorities Blame Taiwan for Cyberattacks, Espionage
- South Korea flags attacks on its drone manufacturers
- Turkey's New Cyber Law Sparks Opposition Concerns
- Hackers Allegedly Target Communications on Iranian Ships
- Hackers Target Malaysia's Airport Systems
- India File

Cyberattack Targets Polish Space Agency, Says Minister

Poland's cybersecurity services have identified unauthorized access to the IT infrastructure of the Polish Space Agency (POLSA), as confirmed by Minister for Digitalization Krzysztof Gawkowski.[1] Officials have not revealed whether ransomware groups or politically motivated hackers conducted the cyberattack. Also, no further details were shared regarding the method used to breach the system. POLSA is the governmental body overseeing the nation's space initiatives. As a member of the European Space Agency (ESA), it plays a key role in Poland's contributions to space exploration and satellite technology.[2]

Cyberattack Hits Russian Telecom Sector, Disruptions Reported

In early March, reports emerged that a targeted distributed denial-of-service (DDoS) attack had disrupted internet services for some Russian users.[3] The attack targeted Beeline, a Moscow-based telecommunications provider, marking the second major cyber assault on the company. Further reports indicate that many Beeline users in Russia experienced difficulties accessing the company's mobile app, while some also encountered website outages, notification failures, and internet disruptions.

In a separate incident, the Ukrainian volunteer hacker group known as the IT Army claimed responsibility for a cyberattack on Russian internet provider Lovit, which disrupted services in Moscow and St. Petersburg for three days.[4] The attack also prevented residents in apartment buildings using Lovit's services from accessing their homes by disabling intercom systems. Furthermore, businesses in the affected buildings reported malfunctions in payment terminals and loyalty programs, according to local media reports.

Massive Outage Hits X, Services Down Worldwide

In early March, the social media platform X experienced intermittent outages, with owner Elon Musk attributing the disruption to an unusually powerful cyberattack.[5] Reports indicated that X was targeted by multiple waves of denial-of-service (DoS) attacks. These attacks overwhelm websites with rogue traffic, causing disruptions. While not always technically sophisticated, they can still lead to significant service interruptions. At the end of March, X experienced another global outage, though this time it lasted only a few hours.[6] This marked yet another disruption for the platform following the earlier DoS attacks reported earlier in the month.

Chinese Authorities Blame Taiwan for Cyberattacks, Espionage

China's Ministry of State Security (MSS) has accused four individuals allegedly connected to Taiwan's military of engaging in cyberattacks and espionage.[7] According to the MSS, the suspects are members of Taiwan's Information, Communications, and Electronic Force Command (ICEFCOM), a unit within the island's defense ministry. Beijing claims that since 2023, ICEFCOM has been carrying out cyber operations targeting critical infrastructure in China, including power grids, water supplies, and telecommunications networks. The MSS

further alleges that the agency has enlisted hackers and cybersecurity firms to assist in government-backed cyber warfare.

South Korea flags attacks on its drone manufacturers

South Korea's intelligence agency has advised local drone companies to implement cybersecurity measures in response to increasing international and state-sponsored hacking attempts.[8] The National Intelligence Service (NIS) issued this recommendation during a recent joint briefing with the transport ministry, emphasizing the need for an anti-hacking security system, according to a press release. The agency also reported that hackers have attempted to breach corporate intranets to steal drone development technologies by using phishing emails and exploiting vulnerabilities in the IT systems of drone firms.

Turkey's New Cyber Law Sparks Opposition Concerns

The Turkish Parliament has passed a contentious cybersecurity law despite strong opposition from politicians, rights groups, and legal experts, who warn it could enable widespread surveillance, restrict free speech, and lead to potential abuses of power.[9] The 21-article legislation, approved by a vote of 246 to 102, introduces new government oversight mechanisms and expands the authority of the Cybersecurity Directorate, established by President Recep Tayyip Erdoğan. One of the most controversial provisions, Article 8, initially sought to grant the head of the Cybersecurity Board sweeping powers to conduct searches, seize data, and duplicate digital records.

Hackers Allegedly Target Communications on Iranian Ships

A hacker group has claimed responsibility for a cyberattack that allegedly disrupted communications on 116 Iranian cargo ships.[10] According to a statement on Telegram, the group, Lab Dookhtegan, timed the operation to coincide with U.S. strikes against Houthi rebels in Yemen. The hackers claimed to have interfered with ship communications, as well as connections between ports and external parties. Iranian authorities have not yet responded to these claims.

Hackers Target Malaysia's Airport Systems

Malaysia Airports Holdings Berhad (MAHB) recently suffered a cyberattack that disrupted its digital systems.[11] The hackers demanded a ransom of $10 million. Prime Minister Anwar Ibrahim confirmed the attack, which took place in late March 2025, during his speech at the Police Day celebration in Kuala Lumpur saying that he refused to pay the $10 million ransom demanded by hackers following the cyberattack.[12]

India File

- The ransomware group Hunters International has published a portion of the data it claims to have stolen from Tata Technologies just over a month after the Indian company confirmed a ransomware attack that led to the suspension of some services.[13] The leaked data, posted on the dark web leak site reportedly includes personal details of some current and former Tata Technologies employees, along with

confidential information such as purchase orders and the company's contracts with clients in India and the United States. The ransomware group claims the dataset consists of over 730,000 documents, including Excel spreadsheets, PowerPoint presentations, and PDF files, amounting to approximately 1.4 terabytes of data.

- Hindustan Aeronautics Limited (HAL) fell victim to a cyber fraud scheme in which scammers, posing as a U.S.-based company, deceived the organization into transferring Rs. 55 lakh.[14] The fraud was uncovered when HAL realized the payment had been sent to the wrong account. The scam came to light after PS Engineering, the intended recipient, reported that they had not received the payment. Upon investigation, HAL discovered that the email ID used in the transaction was fraudulent.

- The total value of digital financial frauds in India reached Rs. 4,245 crore during the first ten months (April–January) of the 2024–25 fiscal year, involving 2.4 million incidents, according to data presented by the Ministry of Finance in the Rajya Sabha.[15] This represents a 67% increase from the Rs. 2,537 crore recorded in 2022–23, which saw 2 million cases. The finance ministry also stated that the Reserve Bank of India (RBI) has implemented the Central Payments Fraud Information Registry, a web-based system for reporting payment-related frauds. Banks, non-bank prepaid payment instrument issuers, and non-bank credit card issuers are required to report such incidents through this platform.

- The first batch of cyber commandos, formed under the Indian Cyber Crime Coordination Centre (I4C), has successfully completed a six-month training program at the Indian Institute of Information Technology (IIIT) in Kottayam.[16] Comprising 30 commandos selected from various state police forces across India, the trainees were chosen through a nationwide entrance exam. They received advanced training in cyber defense strategies, ethical hacking, digital forensics, and penetration testing to strengthen the country's digital security framework.

- India reported 465 incidents of aircraft navigation system interference between November 2023 and February 2025, with most cases occurring near the border regions of Amritsar and Jammu, close to Pakistan.[17] A major concern is GPS spoofing, a technique that involves transmitting counterfeit signals to mislead Global Navigation Satellite Systems (GNSS) receivers. This growing threat poses serious risks to aviation safety, both in India and worldwide.

- A cache of sensitive defense data, including the engineering design of a weapon, details of a new Air Force facility, procurement plans, and India's strategic collaborations with other countries, has allegedly been stolen by a hacker group and put up for sale.[18]

The leaked data reportedly belongs to the Defence Research and Development Organisation (DRDO). According to an analysis by a cybersecurity firm, the information appears to have been stolen from the device of a former Defence Ministry official.

[1] Reuters, Cyberattack detected at Polish space agency, minister says, 3 March 2025, https://www.reuters.com/world/europe/cyberattack-detected-polish-space-agency-minister-says-2025-03-02/

[2] The Record, Polish space agency investigates cyberattack on its systems, 3 March 2025, https://therecord.media/poland-space-cyberattack-agency-investigate

[3] The Record, Russian telecom Beeline facing outages after cyberattack, 3 March 2025, https://therecord.media/russian-telecom-beeline-outages-cyber

[4] The Record, Lengthy disruption of Russian internet provider claimed by Ukrainian hacker group, 25 March 2025, https://therecord.media/russia-isp-lovit-outages-claimed-ukraine-it-army

[5] Reuters, Musk blames X outage on cyberattack, 11 March 2025, https://www.reuters.com/technology/social-media-platform-x-down-thousands-users-downdetector-shows-2025-03-10/

[6] The Hindu, X faces global outage including in India for couple of hours, 31 March 2025, https://www.thehindu.com/news/international/x-faces-global-outage-including-in-india-for-couple-of-hours/article69394476.ece.

[7] The Record, China identifies Taiwanese hackers allegedly behind cyberattacks and espionage, 18 March 2025, https://therecord.media/china-taiwan-hacks-identify-cyber

[8] The Korea Times, Spy agency urges drone firms to establish security system amid hacking attempts, 17 March 2025, https://www.koreatimes.co.kr/southkorea/defense/20250317/south-koreas-spy-agency-urges-drone-firms-to-establish-security-system-amid-hacking-attempts

[9] Turkish Minute, Turkey passes controversial cybersecurity law amid concerns from opposition, 13 March 2025, https://turkishminute.com/2025/03/13/turkey-passes-controversial-cybersecurity-law-amid-concerns-from-opposition123/

[10] TradeWinds, Hackers claim to have disrupted communications on 116 Iranian ships, 21 March 2025, https://www.tradewindsnews.com/tankers/hackers-claim-to-have-disrupted-communications-on-116-iranian-ships/2-1-1795772

[11] The Cyber Express, Cyberattack Hits Malaysia Airports; PM Anwar Rejects $10M Ransom, 26 March 2025, https://thecyberexpress.com/mahb-cyberattack/

[12] Bitdefender, Malaysian PM says "no way" to $10 million ransom after alleged cyber attack against Kuala Lumpur airport, 27 March 2025, https://www.bitdefender.com/en-gb/blog/hotforsecurity/malaysian-pm-says-no-way-to-10-million-ransom-after-alleged-cyber-attack-against-kuala-lumpur-airport

[13] TechCrunch, Tata Technologies' data leaked by ransomware gang, 11 March 2025, https://techcrunch.com/2025/03/11/tata-technologies-data-leaked-by-ransomware-gang

[14] Business Standard, HAL loses Rs 55 lakh in cyber fraud after scammers alter email address, 18 March 2025, https://www.business-standard.com/india-news/hal-loses-rs-55-lakh-in-cyber-fraud-after-scammers-alter-email-address-125031800890_1.html

[15] Business Standard, Online scams drain Rs 4,245 crore in just 10 months, shows govt data, 20 March 2025, https://www.business-standard.com/finance/news/digital-financial-frauds-touch-rs-4-245-crore-in-the-apr-jan-period-of-fy25-125032001214_1.html

[16] The New Indian Express, First batch of cyber commandos completes training at IIIT-Kottayam in Kerala, 26 March 2025, https://www.newindianexpress.com/states/kerala/2025/Mar/26/first-batch-of-cyber-commandos-completes-training-at-iiit-kottayam-in-kerala.

[17] The Eurasian Times, Are Israel's GPS Attacks Impacting India As It Records 465 Incidents Of "GPS Spoofing" In Last 15 Months?, 24 March 2025, https://www.eurasiantimes.com/rising-threat-of-gps-spoofing-in-global-aviation/

[18] India Today, Secret documents, weapon design among sensitive defence data leaked: Report, , 28 March 2025 https://www.indiatoday.in/india/story/secret-documents-weapon-design-among-sensitive-defence-data-leaked-report-2700673-2025-03-28