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

CYBER *Digest*

May 2025

- China Alleges U.S. NSA Cyberattacks Targeted Asian Winter Games
- Germany Probes Suspected Russian Cyberattack on Research Group
- Algerian Hackers Breach Moroccan Government Websites
- Cyberattack Hits Marks & Spencer, a Multinational Retailer
- Ransomware Disrupts Operations at Major Kidney Dialysis Provider
- Europcar Data Breach Exposes 200,000 Customers
- Pakistan-Based Hackers Target Indian Websites Amid Tensions
- India File

China Alleges U.S. NSA Cyberattacks Targeted Asian Winter Games

China has accused the U.S. National Security Agency (NSA) of conducting sophisticated cyberattacks during the Asian Winter Games in February, targeting critical sectors.[1] Police in Harbin, a city in northeast China, reportedly placed three suspected NSA operatives on a wanted list and implicated the University of California and Virginia Tech in the attacks following an investigation, according to state-run Xinhua News Agency. The report did not detail the specific role of the two American universities in the alleged cyberattacks. China's Foreign Ministry later confirmed the incidents and stated that Beijing had formally expressed its concerns to Washington.

Germany Probes Suspected Russian Cyberattack on Research Group

German intelligence officials announced they are investigating a suspected Russian cyberattack targeting the German Association for East European Studies (DGO).[2] The DGO, a foreign policy and international relations think tank, is one of several organizations in Germany labeled "undesirable" by Moscow.[3] Kremlin-linked hackers are also believed to have targeted multiple German political parties using malware. The DGO disclosed the breach in late March, revealing that attackers had accessed its email communications. Suspicion arose when experts noticed repeated access to the group's mail server from an IP address previously linked to a similar incident last year.

Algerian Hackers Breach Moroccan Government Websites

In April, the Algerian hacker group JabaRoot DZ launched a series of cyberattacks on Moroccan institutions, potentially resulting in the country's largest data breach to date.[4] The primary targets were the websites of the Ministry of Economic Inclusion and the National Social Security Fund (CNSS). The group outlined its motivations on its Telegram channel. While the Ministry of Economic Inclusion acknowledged that its website had been defaced by hackers claiming to be Algerian, it downplayed the incident, emphasizing that the site is purely informational and does not contain any sensitive or professional databases. Reports indicate that the stolen data was uploaded to an underground forum on the dark web, though it has not been put up for sale, which suggests that the motive behind the attack may be political rather than financial.[5] Experts pointed out that such tactics are often employed by espionage groups operating under the guise of hacktivists.

Cyberattack Hits Marks & Spencer, a Multinational Retailer

In the final week of April, British retailer Marks & Spencer confirmed it had been dealing with a cyber incident over several days, prompting temporary adjustments to some of its store operations.[6] Marks & Spencer has brought in cybersecurity experts to investigate and contain the incident, stating that it is taking additional measures to strengthen its network security and ensure uninterrupted service for customers.[7] Since news of the cyberattack emerged, Marks & Spencer has seen

approximately £700 million ($930 million) wiped off its stock market value.[8]

Ransomware Disrupts Operations at Major Kidney Dialysis Provider

Kidney dialysis provider DaVita disclosed that a ransomware attack disrupted parts of its operations, encrypting sections of its network.[9] In a filing with the U.S. Securities and Exchange Commission, the company stated it had activated its response protocols, isolated affected systems, and implemented containment measures. DaVita promptly implemented containment measures and isolated the affected systems following the ransomware attack.[10] The company also enlisted third-party cybersecurity experts and notified law enforcement to assist in the investigation and response.

Europcar Data Breach Exposes 200,000 Customers

A hacker breached the GitLab repositories of Europcar Mobility Group, a multinational car rental company, stealing source code for its Android and iOS applications, along with personal data of up to 200,000 customers.[11] The attacker also attempted to extort the company by threatening to release 37GB of data, which included backups and sensitive details about the company's cloud infrastructure and internal applications. While the full scope of the breach is still under assessment, the stolen data appears to be limited to names and email addresses of users from Europcar subsidiaries Goldcar and Ubeeqo. Online data suggests the number of affected individuals ranges from 50,000 to 200,000, with some records dating back to 2017 and 2020.

Pakistan-Based Hackers Target Indian Websites Amid Tensions

Following the Pahalgam terror attack, Pakistani hackers have intensified cyber offensives against Indian websites, particularly those linked to the Indian Armed Forces.[12] The official website of the Army College of Nursing in Punjab was among those targeted and defaced. Hackers also targeted several other Indian defense-related websites, including Army Public School (APS) Srinagar, APS Ranikhet, the Army Welfare Housing Organisation (AWHO) database, and the Indian Air Force Placement Organisation portal.[13] The attacks aimed to deface web pages, disrupt services through a denial-of-service (DoS) attack on APS Srinagar, and gain access to personal data. Reports also highlighted that India successfully thwarted a coordinated cyber offensive launched by Pakistan-based actors.[14]

India File

- Cybercrime police have arrested three individuals for defrauding a private bank by creating a fake state government email ID and sending 18 forged court orders to transfer ₹1.32 crore from two frozen accounts.[15] According to reports, the accused registered the fake government email by submitting false information to the Karnataka State Wide Area Network (KSWAN), which is managed by the state's Centre for e-Governance to provide secure connectivity for government departments. Using this fraudulent email ID, they sent counterfeit court orders to the bank's nodal email address at its Halasuru Gate branch in Bengaluru,

targeting accounts that had been frozen by legitimate court directives. The suspects had sourced information about the frozen accounts through online research, police said.

- Police have uncovered links to a Chinese cyber fraud syndicate operating out of the so-called "Golden Triangle", a region spanning Cambodia, Myanmar, and Laos, in connection with a case involving the swindling of ₹90 lakh from a retired Kerala High Court judge.[16] Kochi Cyber Police have arrested three individuals from Thalassery with ties to the scam. Investigators revealed that the stolen funds were converted into bitcoins and funneled through international entities, eventually tracing back to cybercrime networks based in the region, which has become a major hub for large-scale fraud operations run largely by Chinese nationals.

- India has released its first Digital Threat Report 2024 to bolster cybersecurity in the Banking, Financial Services, and Insurance (BFSI) sector.[17] What sets the 2024 report apart is its comprehensive approach, it not only assesses current threats and emerging vulnerabilities but also explores adversarial tactics that affect system-level operations. The report offers a sector-wide view of security gaps and delivers forward-looking insights into potential cyber risks, enabling financial institutions to better prepare for both present and future threats.

- According to media reports, the website of Nippon Life India Mutual Fund was targeted in a cyberattack.[18] The following day, the company informed stock exchanges about the incident, confirming that its IT infrastructure had been compromised. While no timeline was provided for the website's restoration, the management assured that efforts were underway to resolve the issue promptly.

- India and Australia are in early-stage discussions to establish real-time information sharing to combat cybercrime, amid rising threats from state-backed actors like North Korea targeting critical infrastructure such as power grids and healthcare systems.[19] Brendan Dowling, Australia's Ambassador for Cyber Affairs and Critical Technologies, confirmed in an interview that both nations are showing strong interest in a bilateral treaty focused on data-sharing to strengthen their cybercrime response capabilities.

- Karnataka has become the first state in India to establish a dedicated Cyber Command Centre, setting a national precedent in tackling a wide range of digital threats.[20] This comprehensive centre will address various aspects of cybersecurity and cybercrime, including ransomware, online crimes against women and children, sextortion, digital frauds, deepfakes, identity theft, hacking, data breaches, digital arrests, stalking, and disinformation. It aims to serve as a centralized hub for prevention, response, and outreach in the fight against evolving cyber threats.

[1] Reuters, China accuses US of launching 'advanced' cyberattacks, names alleged NSA agents, 15 April 2025, https://www.reuters.com/technology/cybersecurity/chinas-harbin-says-us-launched-advanced-cyber-attacks-winter-games-2025-04-15/

[2] DW, Germany suspects Russian cyber attack on research group, 8 April 2025, https://www.dw.com/en/germany-suspects-russian-cyber-attack-on-research-group/a-72175406

[3] Ibid.

[4] Yabiladi, Algerian hackers leak sensitive data from Morocco's CNSS and Ministry of Employment, 9 April 2024, https://en.yabiladi.com/articles/details/163560/algerian-hackers-leak-sensitive-data.html

[5] The Record, Morocco investigates major data breach allegedly by Algerian hackers, 11 April 2025, https://therecord.media/morocco-investigates-breach-hackers-algeria

[6] Reuters, British food and clothing group M&S discloses cyber incident, 22 April 2025, https://www.reuters.com/business/retail-consumer/british-retailer-ms-discloses-cyber-incident-2025-04-22/

[7] The Guardian, Marks & Spencer pauses online orders as firm struggles with cyber-attack fallout, 25 April 2025, https://www.theguardian.com/business/2025/apr/25/marks-and-spencer-pauses-online-orders-cyber-attack-fallout

[8] Reuters, Cyberattacks blight Britain's retailers as M&S, Co-op's systems' breached, 3 May 2025, https://www.reuters.com/business/retail-consumer/britains-ms-enters-second-week-sales-disruption-after-cyberattack-2025-05-02/

[9] The Record, Ransomware disrupts some operations of kidney dialysis company DaVita, 14 April 2025, https://therecord.media/davita-kidney-dialysis-company-ransomware-attack

[10] Techtarget, Dialysis firm DaVita suffers ransomware attack, 14 April 2025, https://www.techtarget.com/healthtechsecurity/news/366622499/Dialysis-firm-DaVita-suffers-ransomware-attack

[11] Bleeping Computer, Europcar GitLab breach exposes data of up to 200,000 customers, 4 April 2025, https://www.bleepingcomputer.com/news/security/europcar-gitlab-breach-exposes-data-of-up-to-200-000-customers/

[12] NDTV, Pakistan's Cyber Crimes Continue: Four Indian Websites Hacked, 27 April 2025, https://www.ndtv.com/video/pakistan-s-cyber-crimes-continue-four-indian-websites-hacked-931888#:~:text=Pakistan's%20Cyber%20Crimes%20Continue%3A%20Four%20Indian%20Websites%20Hacked,-2%3A36&text=Now%20after%20the%20Pahalgam%20terror,have%20been%20hacked%20so%20far.

[13] NDTV, Pak-Based Hackers Target Army Public Schools, Other Indian Sites, 29 April 2025, https://www.ndtv.com/india-news/pak-based-hackers-target-army-public-schools-other-indian-sites-8286389

[14] The Times of India, India foils repeated Pakistan attempts to hack Army sites amid tensions, 30 April 2025, https://timesofindia.indiatimes.com/india/india-foils-repeated-pakistan-attempts-to-hack-army-sites-amid-tensions/articleshow/120726974.cms

[15] The New Indian Express, Three create fake govt email ID, transfer Rs 1.32 crore from private bank in Karnataka, 12 April 2025, https://www.newindianexpress.com/states/karnataka/2025/Apr/12/three-create-fake-govt-email-id-transfer-rs-132-crore-from-private-bank-in-karnataka

[16] The New Indian Express, Scamsters from Kerala linked to Chinese fraud network 'Golden Triangle', 6 April 2025, https://www.newindianexpress.com/cities/kochi/2025/Apr/06/scamsters-from-kerala-linked-to-chinese-fraud-network-golden-triangle

[17] Press Information Bureau (PIB), India launches first Digital Threat Report 2024 to support cybersecurity in the Banking, Financial Services and Insurance (BFSI) sector, 7 April 2025, https://pib.gov.in/PressReleasePage.aspx?PRID=2119801

[18] Money Control, Nippon Life India MF website remains offline post-April 9 cyberattack, company working to reinstate availability 'soon', 18 April 2025, https://www.moneycontrol.com/news/business/mutual-funds/nippon-life-india-mf-website-remains-offline-post-april-9-cyberattack-company-working-to-reinstate-availability-soon-12998108.html

[19] Livemint, India, Australia explore bilateral data-sharing treaty to tackle cybercrime, 17 April 2025, https://www.livemint.com/technology/tech-news/india-australia-bilateral-data-sharing-treaty-to-cybercrimes-china-cyberattack-mumbai-power-outage-11744807121725.html

[20] The New Indian Express, Karnataka sets up India's first Cyber Command Centre to combat rising cybercrimes, 10 April 2025, https://www.newindianexpress.com/states/karnataka/2025/Apr/10/karnataka-sets-up-indias-first-cyber-command-centre-to-combat-rising-cybercrimes