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

CYBER *Digest*

July 2026

- Cyberattack Hits Three Iranian Banks
- French Government Messaging Service Compromised
- Defacement Attack Hits Philippine Senate Website
- Five Eyes alliance flags Chinese espionage via recruitment sites
- Dashlane Reports Password Vault Theft
- Australia Launches Phase 2 Of Its Cyber Resilience Plan
- Oxford University Confirms Data Breach Of Its CareerConnect Platform
- KDDI Investigates Possible Leak of 14 Million Email Accounts
- India File

Cyberattack Hits Three Iranian Banks

Iran's state-owned banking technology provider said cyberattacks disrupted card-based banking services at Bank Melli, Bank Saderat, and Bank Tejarat, prompting the temporary suspension of all card-related operations to prevent further unauthorised access.[1] The company said cybersecurity teams were working to restore services, while ATM networks, point-of-sale terminals, and mobile banking applications linked to card systems were affected. Iran's Banking Coordination Council also reported disruptions at several major banks, including Bank Melli, Bank Saderat, Bank Tejarat, and the Export Development Bank of Iran, following a cyberattack targeting a shared banking communication system.

French Government Messaging Service Compromised

France's digital affairs directorate (DINUM) has disclosed that hackers breached Tchap, the French government's encrypted messaging platform, by exploiting a compromised user account.[2] Developed by DINUM in collaboration with ANSSI, France's national cybersecurity agency, Tchap is a secure messaging and collaboration platform based on the decentralised Matrix protocol and is used exclusively across the French public sector. According to DINUM, ANSSI detected the breach after identifying unauthorised access to the platform through the hijacked account.

Defacement Attack Hits Philippine Senate Website

The Philippine Senate has confirmed that its official website was defaced in a cyberattack, with a group calling itself Nullsec Philippines claiming responsibility.[3] The Senate said its technical team immediately activated security protocols and launched an investigation to determine the nature and scope of the unauthorised activity. While additional security measures are being implemented to prevent similar incidents, initial assessments indicate that no confidential or sensitive information was compromised. The affected website primarily hosts publicly accessible documents and informational materials.

Five Eyes Alliance Flags Chinese Espionage Via Recruitment Sites

The Five Eyes intelligence alliance comprising the US, UK, Canada, Australia and New Zealand issued a rare joint warning that Chinese military intelligence is aggressively using professional networking and job-recruitment platforms to target and recruit individuals with access to sensitive government, defence and foreign-policy information, especially across the Indo-Pacific.[4] The bulletin describes how targets are approached under false identities, paid for reports, and gradually pressured to provide classified material, while China's London embassy dismissed the allegations as fabricated and politically motivated.[5]

Dashlane Reports Password Vault Theft

Password manager maker Dashlane has disclosed that hackers obtained at least a dozen encrypted password vaults during a cyberattack.[6] According to the company, attackers bypassed its two-factor authentication system through a brute-force attack, enabling them to access around 20 customer accounts. The breach allowed the attackers to download encrypted vaults

containing users' passwords and other sensitive credentials. Dashlane confirmed that there is no evidence that its internal systems were compromised. Dashlane also said that it has notified the approximately 20 customers whose encrypted password vaults were stolen. The company added that it remains unclear whether the affected individuals were specifically targeted because of their identity, profession, or other factors.

Kodak Discloses Data Breach

Kodak has confirmed it is investigating a cybersecurity breach with the assistance of external experts after attackers gained unauthorised access to a limited amount of company data.[7] While the company has not attributed the incident to any threat actor, the ShinyHunters extortion group has claimed responsibility, alleging it stole more than 2.2 million records containing customer personally identifiable information (PII) and internal corporate data. The group has also threatened to publish the stolen data on its dark web leak site.

Australia Launches Phase 2 Of Its Cyber Resilience Plan

Australia has launched Horizon 2, the next phase of its 2023–2030 Cyber Security Strategy, outlining a 2026–2028 work program aimed at strengthening national cyber resilience. The plan focuses on human-layer vulnerabilities, small-business uplift, supply-chain cyber exercises, and preparation for emerging technological and geopolitical threats.[8]

It sets out 19 actions and 64 initiatives led by 12 government agencies, emphasising the need to build a "human firewall" through workforce resilience and secure adoption of rapidly evolving technologies. Public consultation shaped the program's priorities and highlighted gaps in national preparedness.

Experts noted that sustained funding, regulatory agility and coordinated implementation will be essential as AI accelerates both cyber offence and defence, making resilience more critical than compliance alone.[9]

Oxford University Confirms Data Breach Of Its CareerConnect Platform

The University of Oxford has disclosed a data breach affecting its CareerConnect careers platform after being notified by third-party provider Group GTI of a security incident.[10] The breach exposed users' first and last names, email addresses, and encrypted passwords. CareerConnect, which is also used by other UK universities including King's College London and the University of Manchester, appears to have been targeted to harvest credentials for potential phishing attacks, according to GTI. Oxford said the incident was limited to GTI's systems and that there is no evidence its own university networks were compromised.

KDDI Investigates Possible Leak of 14 Million Email Accounts

Japan's KDDI has disclosed a cyberattack on its email system used by internet service providers, warning that up to 14.22 million email addresses and passwords may have been exposed.[11] The affected providers include STNet, JCOM, Chubu Telecommunications, Nifty, Biglobe, and KDDI Web Communications. According to KDDI, the attackers exploited vulnerabilities in third-party software used

by the email system. The company said it has implemented protective measures, is continuing to investigate the full extent of the breach, and is working with affected service providers to advise users to change their passwords.

India File

- Tata Electronics has confirmed it is investigating a cybersecurity incident after researchers said the World Leaks ransomware group published more than 200,000 files on its dark web leak site, including alleged component design and specification documents linked to Apple and Tesla, both customers of the Indian company.[12] According to a report, Apple is conducting its own analysis, while Tata Electronics has received a ransom demand. A Cybersecurity researcher said that the leaked data also includes emails, event logs spanning several years, and passport copies of employees, including foreign nationals.
- Bajaj Auto Ltd. has disclosed a ransomware attack that affected the IT systems of the company and its wholly owned subsidiary, Bajaj Auto Technology Ltd. (BATL).[13] In a regulatory filing, the Pune-based automaker said its technical team, working alongside external cybersecurity experts and management, responded immediately after detecting the incident and implemented precautionary measures and response protocols to contain the impact. Based on the information currently available, the company said the mitigation efforts have been successful.
- The Ministry of Women and Child Development organised a cybersecurity workshop for its officers to enhance awareness of information security, cyber hygiene, application security, data protection, and safe digital practices.[14] Experts from CERT-In delivered presentations on key cybersecurity issues, while the workshop was attended by Anil Malik, Secretary of the Ministry, and around 120 ministry officials.
- Amit Shah, Union Home Minister and Minister of Cooperation, reviewed the National Cyber Crime Helpline 1930 and directed officials to modernise the system using advanced technologies, including artificial intelligence (AI), to improve its efficiency and response capabilities.[15] During the high-level meeting, he also reviewed citizen-centric mechanisms for providing immediate assistance in cybercrime cases, particularly financial fraud. The minister also emphasised that every complaint should receive timely attention and instructed that the upgraded helpline enable faster complaint registration, intelligent call routing, and more effective grievance management.

[1] Reuters, Iran says card-based banking hit by cyberattack on three lenders, 23 June 2026, https://www.reuters.com/world/middle-east/iran-says-card-based-banking-hit-by-cyberattack-three-lenders-2026-06-23/

[2] Bleeping Computer, French govt messaging service breached in account hijacking attack, 9 June 2026, https://www.bleepingcomputer.com/news/security/french-govt-messaging-service-breached-in-account-hijacking-attack/

[3] The Filipino Times, Senate website hit by defacement attack, security review underway, 11 June 2026, https://filipinotimes.net/latest-news/2026/06/11/senate-website-hit-by-defacement-attack-security-review-underway/

[4] Five Eyes security alliance warns of Chinese espionage threat, 4 June 2026, https://www.reuters.com/business/media-telecom/five-eyes-security-alliance-warns-chinese-espionage-threat-2026-06-03

[5] Five Eyes Joint Bulletin - Safeguarding Our Secrets, 3 June 2026, https://www.mi5.gov.uk/five-eyes-joint-bulletin-safeguarding-our-secrets

[6] TechCrunch, Password manager Dashlane says hackers stole some customers' password vaults, 2 June 2026, https://techcrunch.com/2026/06/02/password-manager-dashlane-says-hackers-stole-some-customers-password-vaults/

[7] Bleeping Computer, Kodak confirms data breach claimed by ShinyHunters extortion gang, 17 June 2026, https://www.bleepingcomputer.com/news/security/kodak-confirms-data-breach-claimed-by-shinyhunters-extortion-gang/

[8] 2023–2030 Australian Cyber Security Strategy, 12 June 2026, https://www.homeaffairs.gov.au/cyber-security-subsite/files/horizon-2-action-plan.pdf

[9] Government launches Horizon 2 action plan for Australia's cyber security strategy, 12 June 2026, https://australiancybersecuritymagazine.com.au/government-launches-horizon-2-action-plan-for-australias-cyber-security-strategy/

[10] Bleeping Computer, Oxford University discloses data breach after careers platform hack, 8 June 2026, https://www.bleepingcomputer.com/news/security/oxford-university-discloses-data-breach-after-careerconnect-platform-hack/

[11] The Japan Times, Information for 14 million email accounts possibly leaked in cyberattack on KDDI, 24 June 2026, https://www.japantimes.co.jp/business/2026/06/24/companies/kddi-data-breach-cyberattack/

[12] Reuters, India's Tata Electronics hit by cyber breach claiming to expose Apple, Tesla trade secrets, 22 June 2026, https://www.reuters.com/business/media-telecom/indias-tata-electronics-hit-by-cyber-breach-claiming-expose-apple-tesla-trade-2026-06-22/

[13] Business Today, What Bajaj Auto ransomware attack says about cyber security risks for Indian automakers, 24 June 2026, https://www.businesstoday.in/auto/story/what-bajaj-auto-ransomware-attack-says-about-cyber-security-risks-for-indian-automakers-538956-2026-06-24

[14] PIB, Ministry of Women and Child Development organises Cyber Security Awareness Workshop, 15 June 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2273491&reg=48&lang=1

[15] PIB, Union Home Minister and Minister of Cooperation Shri Amit Shah reviews National Cyber Crime Helpline 1930 and directs to make it better, 17 June 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2274249&reg=48&lang=1