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

CYBER *Digest*

June 2026

- **Australia Launches Cyber Review Board**
- **Hackers Breach Vietnamese Ministry Systems**
- **Lithuania Probes Theft of State Records by Foreign Actor**
- **Claude Used in Attempted Hack of Mexican Water Utility**
- **France Probes Israeli Firm Over Alleged Election Interference**
- **MENA Cybercrime Crackdown Leads to 201 Arrests**
- **WFP Cyberattack Exposes Gaza Household Data**
- **Sri Lanka Arrests Chinese Nationals in Suspected Scam Operation**
- **India File**

Australia Launches Cyber Review Board

Australia has formally established a Cyber Incident Review Board to carry out post-incident assessments of major cybersecurity breaches, with the aim of identifying actionable lessons and enhancing national cyber resilience.[1] The board will review significant cyber incidents and issue recommendations to both government and industry on improving the prevention, detection, response, and mitigation of future cyberattacks. Created under the Cyber Security Act 2024, the initiative is a key component of Australia's 2023–2030 Cyber Security Strategy and reflects the country's broader ambition to become one of the world's most cyber-secure nations by the end of the decade.

The seven-member board comprises experienced cybersecurity leaders from industry, academia, and critical infrastructure sectors, bringing together expertise in technology, governance, and national security to provide independent guidance. Its core mandate is to systematically analyse and learn from major cyber incidents, reflecting a broader shift towards greater operational accountability and continuous improvement across the national cybersecurity ecosystem.

Hackers Breach Vietnamese Ministry Systems

According to reports, Vietnam in the last week of May was responding to two major data breaches affecting ministerial-level agencies, where hackers reportedly accessed systems containing millions of user records.[2] Initial investigations by VNCERT found that although the affected agencies had Security Operations Centre (SOC) platforms in place, the attacks went undetected. Authorities are investigating whether the malicious activity was disguised as normal user behaviour, with VNCERT expected to release its findings soon.

Lithuania Probes Theft of State Records by Foreign Actor

Lithuanian authorities have disclosed a major data breach affecting state registry systems, with more than 600,000 records reportedly accessed without authorisation.[3] According to the Prosecutor General's Office, attackers exploited login credentials belonging to institutions authorised to use the databases, with the intrusion believed to have originated from a foreign country. The breach impacted the Real Estate and Legal Entities Registers, exposing personal data such as names, dates of birth, and national identification numbers, as well as property-related information, including addresses, and registry records.

Claude Used in Attempted Hack of Mexican Water Utility

An unidentified cyber threat group reportedly used Anthropic's Claude AI to support a sophisticated intrusion attempt against a local water utility in Mexico as part of a broader campaign targeting nine federal, state, and municipal government agencies between December 2025 and February 2026.[4] According to a report, the attackers leveraged AI tools extensively after compromising IT systems, despite having little prior knowledge of the targeted environment. While they failed to breach the operational technology (OT) network, the incident highlights the growing use of generative AI to accelerate cyber operations against critical infrastructure.

France Probes Israeli Firm Over Alleged Election Interference

French prosecutors have launched an investigation into allegations that an Israeli company interfered in local elections through coordinated disinformation campaigns.[5] The probe follows complaints from three members of the far-left La France Insoumise, who claim they were targeted with false accusations, manipulated social media activity, and fabricated campaign materials. The investigation was prompted by findings from France's online disinformation watchdog, which identified a network of automated and artificial dissemination used to spread misleading content. Authorities said the campaign, allegedly orchestrated by an actor based abroad, may have undermined citizens' access to accurate information and threatened the nation's fundamental interests.

MENA Cybercrime Crackdown Leads to 201 Arrests

A landmark cybercrime crackdown across the Middle East and North Africa (MENA) has resulted in the arrest of 201 individuals and the identification of 382 additional suspects.[6] Conducted between October 2025 and February 2026, Operation Ramz involved 13 countries and targeted phishing campaigns, malware operations, and online fraud schemes. The operation led to the identification of 3,867 victims and the seizure of 53 servers. Coordinated by INTERPOL, Operation Ramz was the first cybercrime operation of its scale in the MENA region, with nearly 8,000 intelligence and data leads shared among participating countries to support investigations and disrupt malicious infrastructure.

WFP Cyberattack Exposes Gaza Household Data

A cyberattack on the World Food Programme (WFP) has exposed sensitive personal data belonging to approximately 600,000 households in Gaza, potentially making it the largest known breach of humanitarian beneficiary information to date.[7] WFP confirmed it is investigating a security incident in which unauthorised actors gained access to personal data submitted by Palestinians in Gaza. The agency disclosed the breach in a statement sent to aid recipients via Telegram on 31 May.

Sri Lanka Arrests Chinese Nationals in Suspected Scam Operation

Sri Lankan authorities have arrested 37 Chinese nationals suspected of operating a cyber scam centre in Colombo as part of an ongoing crackdown on foreign-run online fraud networks.[8] The suspects, aged between 23 and 44, had reportedly entered the country on tourist visas and were working illegally, while two were found to have overstayed their visas. Following a tip-off, police raided the facility and seized 35 tablet computers, 147 mobile phones, and 100 SIM cards from the suspected scam operation in a Colombo suburb.

India File

- India and South Korea have signed agreements to strengthen cooperation in defence, cyber security, military training, and UN peacekeeping.[9] The pacts include collaboration in defence cyber affairs and training exchanges between India's National Defence College and South Korea's Korea National Defence University. The

agreements were exchanged during talks in Seoul between Indian Defence Minister Rajnath Singh and South Korean Defence Minister Ahn Gyu-back. Both sides also discussed expanding cooperation in the defence industry, maritime security, emerging technologies, military exchanges, logistics, and regional security, while reaffirming their commitment to a free and rules-based Indo-Pacific.

- India's anti-cybercrime agency, the Indian Cyber Crime Coordination Centre (I4C), has signed an MoU with the Reserve Bank Innovation Hub to tackle mule accounts used by cybercriminals for financial fraud.[10] The partnership will facilitate fraud-risk intelligence sharing, analytical support, and operational coordination to strengthen proactive fraud detection and prevention across financial institutions.
- The Election Commission of India successfully mitigated over 6.8 million malicious cyber attacks targeting its ECINET portal during vote counting for the assembly elections in West Bengal, Tamil Nadu, Assam, Kerala, and Puducherry.[11] While the ECINET website and mobile application provided real-time election results to the public, the platform also served as a critical operational tool for election officials, underscoring the importance of its cyber resilience during the electoral process.
- The Ministry of Electronics and Information Technology (MeitY) convened a National Consultative Workshop on "Strengthening Cyber Security Frameworks for State Data" on 11 May 2026.[12] The workshop brought together senior officials from all States and Union Territories, along with representatives from the Indian Computer Emergency Response Team, National Informatics Centre, MeitY, and the National e-Governance Division. Conducted in partnership with NeGD, the initiative aims to develop a comprehensive national cybersecurity policy framework for State governments through structured consultations with all 36 States and Union Territories.
- The investigation into a Rs. 24-crore digital arrest scam targeting a 74-year-old retired teacher in Bengaluru has expanded, with the Karnataka State Cyber Command uncovering connections between the accused and several cyber fraud cases across India, including a Rs. 15-crore fraud case in Belagavi.[13] According to the Cyber Command Unit, two of the arrested suspects were also allegedly involved in a separate digital arrest scam registered at the CEN Crime Police Station in Belagavi, where victims were defrauded of nearly Rs. 15 crore. The findings suggest the existence of a wider cyber fraud network operating across multiple states.

[1] Industrial Cyber, Australia sets up Cyber Incident Review Board to learn from cyberattacks, build continuous cyber resilience, 7 May 2026, https://industrialcyber.co/threat-landscape/australia-sets-up-cyber-incident-review-board-to-learn-from-cyberattacks-build-continuous-cyber-resilience/

[2] Vietnam Net, Hackers breach two Vietnamese ministerial systems in major cyberattack, 22 May 2026, https://vietnamnet.vn/en/hackers-breach-two-vietnamese-ministerial-systems-in-major-cyberattack-2518404.html

[3] The Record, Lithuania investigates theft of 600,000 state registry records by foreign actor, 26 May 2026, https://therecord.media/lithuania-investigates-theft-of-state-records

[4] Cybersecurity Dive, Anthropic's Claude used in attempted compromise of Mexican water utility, 8 May 2026, https://www.cybersecuritydive.com/news/anthropics-claude-compromise-mexican-water-utility/819710/

[5] The Times of Israel, France probes alleged local election interference by Israeli company, 27 May 2026, https://www.timesofisrael.com/france-probes-alleged-local-election-interference-by-israeli-company/

[6] Interpol, 201 arrests in first-of-its-kind cybercrime operation in MENA region, 18 May 2026, https://www.interpol.int/en/News-and-Events/News/2026/201-arrests-in-first-of-its-kind-cybercrime-operation-in-MENA-region

[7] The New Humanitarian, Data of 600,000 Gaza households exposed in WFP cyber-attack, 2 June 2026, https://www.thenewhumanitarian.org/news/2026/06/02/data-600000-gaza-households-exposed-wfp-cyber-attack

[8] The Straits Time, Sri Lanka arrests 37 Chinese at suspected scam centre: Police, 3 May 2026, https://www.straitstimes.com/asia/south-asia/sri-lanka-arrests-37-chinese-at-suspected-scam-centre-police

[9] NDTV, India, South Korea Sign Pact On Defence, Cyber, Training Cooperation, 21 May 2026, https://www.ndtv.com/india-news/india-south-korea-sign-pact-on-defence-cyber-training-cooperation-11525565

[10] The New Indian Express, Amit Shah announces MoU between anti-cyber crime agency, RBI's innovation hub to curb mule accounts, 12 May 2026, https://www.newindianexpress.com/india/2026/May/12/union-minister-amit-shah-announces-mou-between-anti-cyber-crime-agency-14c-rbih-to-curb-mule-accounts

[11] The Indian Express, Thwarted 68 lakh cyber attacks on ECINET portal on counting day: Election Commission, 7 May 2026, https://indianexpress.com/article/india/ecinet-portal-cyberattack-election-commission-68-lakh-malicious-hits-2026-results-10676447/

[12] PIB, National Consultative Workshop on "Strengthening Cyber Security Frameworks for State Data", 16 May 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2261823&reg=48&lang=2

[13] The Indian Express, Rs 24-crore 'digital arrest' scam probe in Bengaluru reveals accused's link to cases nationwide, 26 May 2026, https://indianexpress.com/article/cities/bangalore/bengaluru-digital-arrest-scam-rs-24-crore-cyber-fraud-interstate-links-10709203/