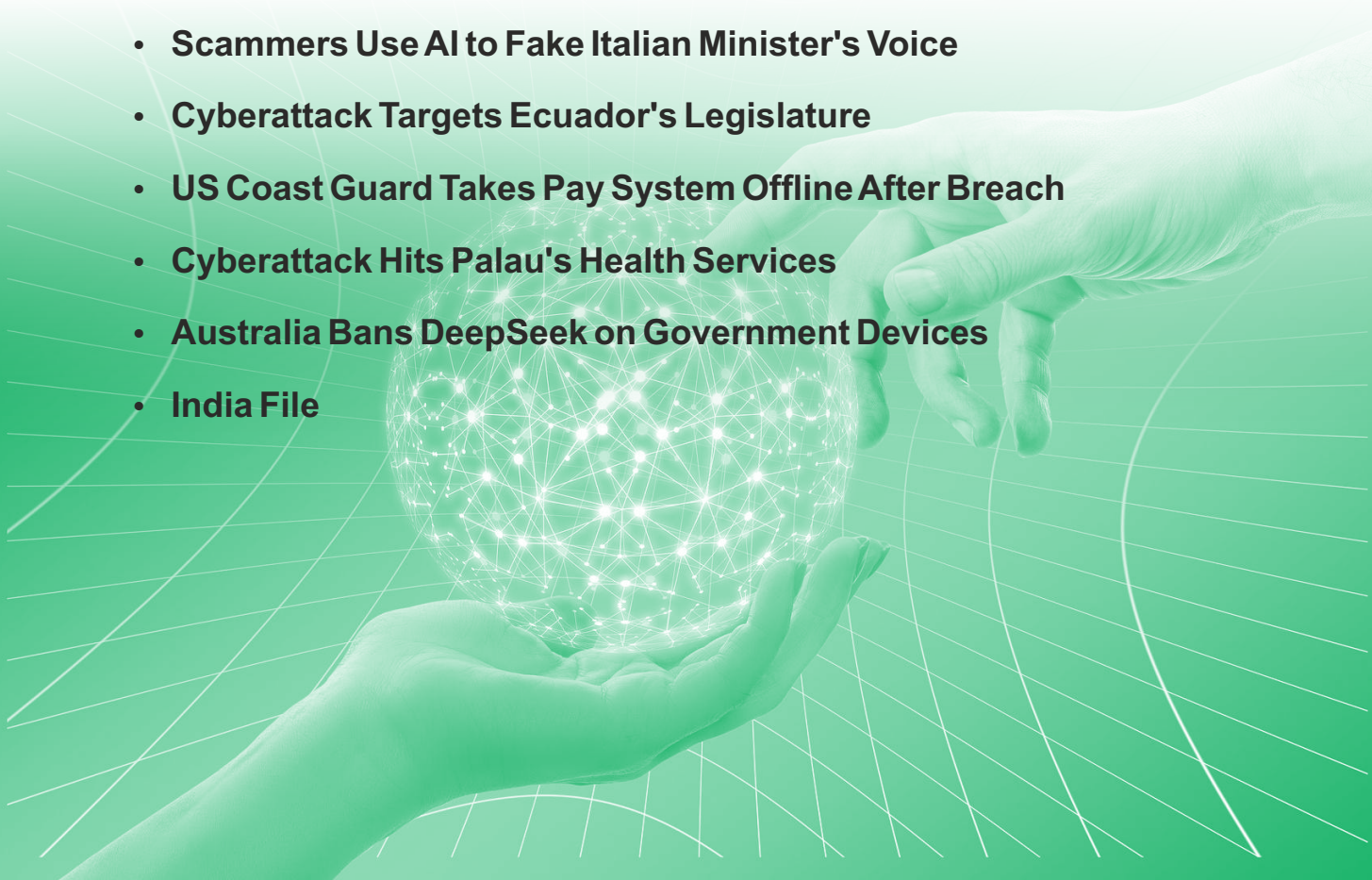
MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

March 2025

- South-East Asia Crackdown on Scam Centers
- Hackers Leak Taliban Records After Cyber Breach
- Japan's Cabinet Approves Cybersecurity Bill
- Scammers Use AI to Fake Italian Minister's Voice
- Cyberattack Targets Ecuador's Legislature
- US Coast Guard Takes Pay System Offline After Breach
- Cyberattack Hits Palau's Health Services
- Australia Bans DeepSeek on Government Devices
- India File



South-East Asia Crackdown on Scam Centers

Thailand has decided to cut the electricity supply to certain border areas with Myanmar to combat scam centers, responding to increasing pressure on these illegal compounds that have trapped numerous individuals of various nationalities.[1] The United Nations reports that criminal gangs have trafficked hundreds of thousands across Southeast Asia, forcing them into fraudulent online operations, including those near the Thai-Myanmar border.

In a separate incident, the Philippine National Bureau of Investigation (NBI) raided an alleged "love scam" operation in a Makati condominium, apprehending up to 100 Filipinos and a Chinese national.[2] NBI Director Jaime Santiago revealed that the suspects leveraged artificial intelligence (AI) to carry out online romance scams. Leading the raid, Santiago stated that agents uncovered the use of AI-generated conversations and fake profile pictures of attractive women to deceive victims into fraudulent cryptocurrency schemes.

Hackers Leak Taliban Records After Cyber Breach

According to reports, the Taliban's Ministry of Communications has confirmed a major cyber breach involving leaked documents from multiple government departments.[3] According to the ministry, initial investigations indicate that the documents were accessed sporadically from individual computers with inadequate security measures. However, Taliban officials insist that their central government database remains secure and unaffected.

A group known as TabiLeaks has shared links on social media to a trove of documents it claims to have exfiltrated from 21 Taliban ministries and government agencies.[4] The leaked records allege that the Taliban has imprisoned over 1,400 women and 16,000 men, along with approximately 80 foreign nationals, including six women.

Japan's Cabinet Approves Cybersecurity Bill

The Japanese Cabinet has approved two bills on "active" cyber defense, enabling Japan to develop preemptive capabilities against cyberattacks.[5]The new measures focus on enhancing cooperation and information-sharing between public and private entities, allowing the government to monitor data traffic within Japan and infiltrate cyberattack sources to neutralize threats. If passed, the bills would expand government authority to protect critical infrastructure and mandate private-sector entities to report acquisitions of critical infrastructure and potential cyberattacks. The collected information would be shared with relevant stakeholders to enhance cybersecurity coordination.

Scammers Use AI to Fake Italian Minister's Voice

A scam involving an AI-generated voice impersonating Italy's Defence Minister Guido Crosetto targeted some of the country's top tycoons, urging them to transfer money overseas. According to Italian media reports, victims included fashion designer Giorgio Armani, former Inter Milan owner Massimo Moratti, Prada co-founder Patrizio Bertelli, and members of the billionaire Beretta and Menarini families, among others. The scammers,

posing as Crosetto and his staff, made phone calls requesting around €1 million to be sent to a Hong Kong-based bank account, claiming the funds were needed to secure the release of kidnapped Italian journalists in the Middle East.

Cyberattack Targets Ecuador's Legislature

Ecuador's National Assembly reported experiencing two cyberattacks, targeting its systems and attempting to access sensitive data. In a statement, the assembly said it swiftly "identified and counteracted the situation" but did not disclose details about the attack's impact or the perpetrators involved.[6] The National Assembly warned that the attacks were aimed at breaching confidential information and urged citizens and public institutions to stay vigilant. It also pledged to take all necessary measures to safeguard sensitive data.

US Coast Guard Takes Pay System Offline After Breach

The U.S. Coast Guard's personnel and pay system was taken offline following a data breach affecting over 1,100 members.[7] Officials confirmed that the service's Direct Access system, which handles payroll and personnel matters, was hacked, exposing sensitive data such as bank routing numbers and direct deposit information. The breach was discovered when an officer noticed unusual activity in their pay account and reported it to Coast Guard Cyber Command, which promptly shut down the system to protect all accounts.

Cyberattack Hits Palau's Health Services

The Qilin ransomware-as-a-service group claimed responsibility for hacking the Palau Ministry of Health and Human Services (MHHS) in a leak post dated February 20.[8] Palau officials later confirmed that the February 17 ransomware attack, carried out by hackers linked to the Qilin group, enabled the attackers to steal files from IT systems used by the MHHS.[9] Government officials contained the incident and restored hospital operations to normal within 48 hours with assistance from Palauan and Australian cybersecurity experts, along with officials from the Ministry of Finance.

Australia Bans DeepSeek on Government Devices

Australia has banned DeepSeek from all government devices and systems, citing national security risks posed by the Chinese AI startup.[10] The government emphasized that the decision was not based on DeepSeek's Chinese origins but on the "unacceptable risk" it presents. The ban requires all government entities to prevent the use or installation of DeepSeek products, applications, and web services, as well as to remove any existing installations from government systems and devices. As a result, employees across various sectors, including the Australian Electoral Commission and the Bureau of Meteorology, will no longer be able to use the tools.

India File

- Telangana's IT Minister, D. Sridhar Babu, announced that the state government will soon introduce a cybersecurity policy aligned with India's Digital Personal Data Protection Act.[11] Speaking at the Cyber Security Conclave 2025, he highlighted Telangana's proactive approach to building a robust

cybersecurity ecosystem and countering cyber threats. The government is also in talks to establish a Cyber Defence Centre in Hyderabad to protect both citizens and government entities from cyber risks.

- Shares of Angel One dropped nearly 4% after the company revealed that some of its Amazon Web Services (AWS) resources were compromised in a data leak, based on alerts from its dark-web monitoring partner.[12] In a regulatory filing, Angel One stated that it was notified via email on February 27 about unauthorized access leading to the data breach. An internal investigation later confirmed the compromise of certain AWS resources.
- A cybersecurity intelligence firm has uncovered a mobile malware campaign involving nearly 900 malware samples, primarily targeting customers of Indian banks.[13] Analysis of the samples indicates a coordinated effort by a single threat actor, as they share code structures, user interface elements, and app logos. Unlike traditional banking Trojans that rely solely on command-and-control (C&C) servers to steal one-time passwords (OTPs), this malware campaign uses live phone numbers to redirect SMS messages, creating a traceable digital trail for law enforcement to track the perpetrators.
- The Indian government has canceled three contracts from domestic drone manufacturers Garuda Aerospace, Dhaksha Unmanned Systems, a unit of Coromandel International, and Sky Industries for procuring 400 logistics drones for the army following reports of hacking incidents involving drones with Chinese components near the international border.[14] The decision marks a major crackdown on domestic private sector firms supplying drones with Chinese parts to the armed forces. Reports highlight that such drones pose a serious cybersecurity threat, increasing the risk of data breaches and compromised military operations.[15]
- Days after a Distributed Denial of Service (DDoS) attack disrupted Karnataka's Kaveri 2.0 portal, which facilitates property registrations, Inspector General of Registrations and Commissioner of Stamps (IGR & CS) K. A. Dayananda formally filed a complaint with the cybercrime police.[16] The attack severely impacted the portal, causing a significant drop in registrations on February 1 and 4. However, services were fully restored by February 5.

[1] Reuters, Thailand to cut power to Myanmar border areas linked to scam centres, 5 February 2025, https://www.reuters.com/world/asia-pacific/thailand-cut-power-myanmar-border-areas-linked-scam-centres-2025-02-04/

[2] Philstar, NBI raids 'love scam' hub in Makati; 100 nabbed, 5 February 2025, https://www.philstar.com/nation/2025/02/05/2419221/nbi-raids-love-scam-hub-makati-100-nabbed

[3] Afghanistan International, Taliban Confirms Data Breach Amidst Major Cyberattack, 6 February 2025, https://www.afintl.com/en/202502062594

[4] Bitdefender, Secret Taliban records published online after hackers breach computer systems, 8 February 2025, https://www.bitdefender.com/en-gb/blog/hotforsecurity/taliban-records-online-hackers-breach

[5] The Japan Times, Japan's Cabinet approves legislation on 'active' cybersecurity, 7 February 2025, https://www.japantimes.co.jp/news/2025/02/07/japan/politics/active-cyber-defense-bill/

[6] The Record, Ecuador's legislature says hackers attempted to access confidential information, 18 February 2025, https://therecord.media/ecuador-national-assembly-cyberattack

[7] Military.com, Data Breach Prompts Coast Guard to Take Personnel and Pay System Offline, 17 February 2025, https://www.military.com/daily-news/2025/02/17/data-breach-prompts-coast-guard-take-personnel-and-pay-system-offline.html.

[8] Cyberdaily.au, Qilin ransomware gang claims hack of Palau Ministry of Health and Human Services, 21 February 2025, https://www.cyberdaily.au/security/11749-exclusive-qilin-ransomware-gang-claims-hack-of-palau-ministry-of-health-and-human-services

[9] The Record, Palau health ministry on the mend after Qilin ransomware attack, 4 March 2025, https://therecord.media/palau-health-ministry-ransomware-recover

[10] BBC, Australia bans DeepSeek on government devices over security risk, 4 February 2025, https://www.bbc.com/news/articles/c8d95v0nr1yo

[11] Telangana Today, Telangana to soon launch Cyber Security policy, says IT Minister Sridhar Babu, 18 February 2025, https://telanganatoday.com/telangana-to-soon-launch-cyber-security-policy-says-it-minister-sridhar-babu

[12] Money Control, Angel One's AWS resources compromised in data leakage; shares fall sharply, 28 February 2025, https://www.moneycontrol.com/news/business/stocks/angel-one-s-aws-resources-compromised-in-data-leakage-sending-shares-lower-by-over-4-12953016.html

[13] Security Boulevard, Mobile Indian Cyber Heist: FatBoyPanel And His Massive Data Breach, 5 February 2025, https://securityboulevard.com/2025/02/mobile-indian-cyber-heist-fatboypanel-and-his-massive-data-breach/

[14] Firstpost, After hacking incidents at border, India scraps deal for 400 drones with Chinese parts, 7 February 2025, https://www.firstpost.com/india/drone-deal-cancelled-scrapped-chinese-parts-army-hacking-at-border-lac-loc-china-pakistan-13860513.html

[15] India Today, Chinese threat in Indian drones, 4 February 2025, https://www.indiatoday.in/magazine/defence/story/20250210-chinese-threat-in-indian-drones-2672839-2025-01-31

[16] The Hindu, Case booked over DDoS attack on Kaveri 2.0, 7 February 2025, https://www.thehindu.com/news/cities/bangalore/case-booked-over-ddos-attack-on-kaveri-20/article69192774.ece