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

CYBER *Digest*

January 2026

- France's Interior Ministry Hit by Major Cyberattack
- Germany Summons Russian Envoy Over Cyberoperations
- Israel Military Bans Android Amid Targeted Cyberattacks
- Asus Confirms Ransomware Attack
- Eight Chinese Nationals Remanded in Pakistan's Online Fraud Case
- Ukrainian Hackers Disrupt Major Russian Logistics Firm
- Korean Air Breach Exposes Thousands of Employees' Records
- India File

France's Interior Ministry Hit by Major Cyberattack

France's Interior Ministry has suffered a cyberattack that compromised official email accounts and exposed sensitive police files, Interior Minister Laurent Nuñez said, adding that a judicial investigation is underway to swiftly identify the perpetrator.[1] The breach occurred after attackers accessed professional inboxes and obtained login credentials; while the full extent is still unclear, officials believe several dozen files may have been exfiltrated. No ransom demand has been received, and the minister attributed the incident to lapses in adherence to security procedures at the French Interior Ministry.

Germany Summons Russian Envoy Over Cyberoperations

Germany summoned the Russian ambassador over allegations of sabotage, cyberattacks, and election interference, a spokesperson for the German Foreign Ministry confirmed.[2] Berlin believes Russia was behind a major cyberattack on Germany's air traffic control systems in August 2024 and has formally attributed the cyberattack to APT28, also known as Fancy Bear, a hacker group linked to Russia's military intelligence agency, the GRU. Alongside the cyberattacks, security agencies detected a targeted disinformation campaign during Germany's snap federal elections in February, which Western security and IT experts have attributed to Storm-1516, a state-controlled group linked to Russia that deliberately spread false information about senior German politicians.

Israel Military Bans Android Amid Targeted Cyberattacks

The Israel Defense Forces is set to tighten mobile device rules for senior officers, banning Android phones on IDF-issued lines and allowing only Apple iPhones for official use by commanders ranked lieutenant colonel and above, Army Radio reported.[3] The move aims to reduce the risk of intrusions by standardising operating systems to strengthen security controls and updates, amid long-standing warnings that hostile actors exploit social media and messaging apps, such as Hamas' alleged use of WhatsApp to target soldiers and track troop movements.

Asus Confirms Ransomware Attack

Asustek Computer Inc., a major Taiwanese electronics company, said one of its suppliers was hacked, leading to the exposure of image-processing source code used in some of its mobile phone cameras.[4] While the company did not identify the attacker, the disclosure followed earlier reports that the Everest gang claimed to have breached Asus and stolen more than 1 terabyte of data, including camera source code. The company declined to validate Everest's broader claims, saying the breach was limited to an unnamed supplier whose systems hosted camera-related code, and has not clarified whether the data involved was proprietary Asus material or belonged to other firms cited by the group.[5]

Eight Chinese Nationals Remanded in Pakistan's Online Fraud Case

Pakistan's National Cyber Crime Investigation Agency has arrested several suspects, including Chinese nationals, for allegedly operating a fraudulent Ponzi scheme network, registering cases under the Prevention of Electronic Crimes Act and the Pakistan Penal Code.[6] Acting on a tip-off, investigators raided a call centre suspected of running online fraud, detaining those who failed to produce legal

authorisation, and alleged that the group used social media advertisements to lure victims into investing funds that were then channelled through multiple bank accounts to fabricate investment growth and profits.

Ukrainian Hackers Disrupt Major Russian Logistics Firm

A cyberattack attributed to Ukraine's military intelligence, the HUR, and the hacktivist BO Team has severely disrupted operations at Russian logistics firm Eltrans+, with reports saying more than 700 systems were hit, over 1,000 user accounts wiped, and 165 TB of data encrypted or destroyed.[7] The incident follows a string of Ukrainian cyber operations, including a recent DDoS attack on Russia's SPB payment system and telecom operator TransTeleCom.

Korean Air Breach Exposes Thousands of Employees' Records

Korean Air disclosed a data breach affecting thousands of employees after its in-flight catering supplier and former subsidiary, Korean Air Catering & Duty-Free, was hacked.[8] While the airline did not specify the number of affected staff, reports indicate that around 30,000 records may have been exfiltrated; the incident has been reported to authorities, and employees have been warned to watch for phishing messages impersonating the company.

India File

- India's Central Bureau of Investigation has busted a transnational cyber fraud ring that allegedly cheated U.S. nationals of $8.5 million (about Rs. 71 crore) through a fake call centre in Noida, in a joint operation with the Federal Bureau of Investigation under Operation Chakra.[9] The CBI arrested six Indian nationals, seized Rs. 1.88 crore in cash, electronic devices, and documents, and said the accused posed as officials from U.S. agencies including the Drug Enforcement Administration, FBI, and Social Security Administration to threaten victims with asset freezes over fabricated investigations, coercing them into transferring funds to crypto wallets or foreign bank accounts controlled by the scammers.
- Coinbase CEO Brian Armstrong said an ex-employee had been arrested in India, months after the company disclosed a data breach involving stolen customer information, thanking the Hyderabad Police without detailing the individual's role in the incident.[10] Coinbase had revealed that cybercriminals bribed rogue overseas support agents to steal customer data in a social engineering attack, with a filing to the Office of the Maine Attorney General putting the number of affected users at 69,461.
- India's Department of Telecommunications has directed messaging platforms including WhatsApp, Telegram, and Signal to enforce SIM binding, requiring services to remain linked to the original SIM via its IMSI, failing which access will be blocked 90 days after the order.[11] As part of the same directive, web versions such as WhatsApp Web will automatically log users out at least every six hours, requiring re-authentication through a QR code scan from the linked phone, a move that has drawn mixed reactions.
- The Government of India has withdrawn a directive requiring smartphone makers to preload the Sanchar Saathi cybersecurity app on new devices, following backlash from opposition

parties, privacy advocates, and global tech firms over surveillance concerns.[12] The rollback came a day after ministers defended the plan as a tool to track stolen phones and protect users from cyber threats.

- India's Indian Computer Emergency Response Team (CERT-In) under the Ministry of Electronics and Information Technology, in collaboration with the Ministry of External Affairs, hosted a cybersecurity familiarisation and interactive session for visiting journalists from Europe, the Americas, and Central Asia.[13] The session highlighted CERT-In's continuous cyber drills, capacity-building efforts, and international cooperation including joint exercises and work with France's ANSSI on a high-level AI cyber risk report titled "Building Trust in AI Through a Cyber Risk-Based Approach."

[1] Euronews, French interior ministry targeted in massive cyberattack, minister confirms, 17 December 2025, https://www.euronews.com/2025/12/17/french-interior-ministry-targeted-in-massive-cyberattack-minister-confirms

[2] Euronews, Germany summons Russian ambassador over alleged election interference and cyberattacks, 12 December 2025, https://www.euronews.com/2025/12/12/germany-summons-russian-ambassador-over-alleged-election-interference-and-cyberattacks

[3] The 420, Israel's Military Bans Android Devices as Targeted Cyberattacks Intensify, Orders To Use Only Iphones, 4 December 2025, https://the420.in/israel-android-ban-iranian-cyber-espionage-military-mobile-security/

[4] Focus Taiwan, Asus confirms ransomware attack on mobile phone camera code, 4 December 2025, https://focustaiwan.tw/sci-tech/202512040005

[5] The Register, Asus supplier hit by ransomware attack as gang flaunts alleged 1 TB haul, 5 December 2025, https://www.theregister.com/2025/12/05/asus_supplier_hack/

[6] Dawn, Eight Chinese nationals among 22 remanded in online fraud case, 21 December 2025, https://www.dawn.com/news/1962349

[7] SC Media, Russian logistics giant taken down by Ukrainian hackers, 9 December 2025, https://www.scworld.com/brief/russian-logistics-giant-taken-down-by-ukrainian-hackers

[8] Bleeping Computer, Korean Air data breach exposes data of thousands of employees, 29 December 2025, https://www.bleepingcomputer.com/news/security/korean-air-data-breach-exposes-data-of-thousands-of-employees/

[9] The 420, CBI Dismantles Cross-Border Cyber Fraud Network Targeting Americans, 12 December 2025, https://the420.in/cbi-noida-cyber-fraud-us-nationals-operation-chakra-fbi/

[10] The Hindu, Coinbase CEO says ex-employee arrested in India, 29 December 2025, https://www.thehindu.com/sci-tech/technology/coinbase-ceo-says-ex-employee-arrested-in-india/article70448478.ece

[11] The Economic Times, Why your WhatsApp Web may now log out every six hours, 1 December 2025, https://economictimes.indiatimes.com/tech/technology/why-your-whatsapp-web-may-now-log-out-every-six-hours/articleshow/125689631.cms?from=mdr

[12] The Indian Express, India revokes order to preload cybersecurity app on smartphones after outcry, 4 December 2025, https://indianexpress.com/article/technology/tech-news-technology/india-revokes-order-to-preload-cybersecurity-app-on-smartphones-after-outcry-10400307/

[13] PIB, CERT-In hosts visiting foreign journalists for an interaction on India's cybersecurity framework, 13 December 2025, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2203387&reg=3&lang=1