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

CYBER *Digest*

March 2026

- France Data Breach Hits Banks and Healthcare
- Cyberattacks Target Italy's Interior Ministry Over Chinese Dissidents
- Senegal Confirms Ransomware Breach at National ID Department
- Norway Says It Was Targeted in Salt Typhoon Cyber Campaign
- Leak Shows China Rehearsed Cyberattacks Abroad
- Korea, Malaysia Police Step Up Cooperation Against Transnational Scams
- Ukraine Says Cyberattacks on Energy Grid Used to Guide Missile Strikes
- Home Minister outlines cybersecurity intiatives and enforcement actions
- India File

France Data Breach Hits Banks and Healthcare

France's Economy Ministry confirmed that a hacker accessed a national database of bank accounts, viewing information linked to 1.2 million accounts.[1] Using stolen credentials belonging to a government official, the attacker was able to consult records covering all bank accounts held in French banks. The compromised data included personal details such as account numbers, account holders' names and addresses, and, in some cases, tax identification numbers. The ministry stated that once the breach was detected, immediate steps were taken to block the unauthorized access and prevent any extraction of data.

France's Health Ministry also confirmed that administrative records and medical notes relating to more than 15 million people were compromised in a cyberattack.[2] The breach reportedly affected millions, including senior political figures, and some of the exposed data has since appeared online. According to the ministry, the leaked information included highly sensitive details, such as patients' sexual orientation and medical conditions, including HIV/AIDS.

Cyberattacks Target Italy's Interior Ministry Over Chinese Dissidents

Italian police confirmed they had identified cyberattacks targeting the Interior Ministry, aimed at obtaining information on Chinese dissidents and officers investigating Chinese groups in Italy.[3] In a statement, police said no sensitive operational data appears to have been compromised. The report said Chinese hackers obtained a list of around 5,000 police officers, many of whom were serving in sensitive roles, including counter-terrorism and monitoring Chinese dissidents in Italy.

Senegal Confirms Ransomware Breach at National ID Department

A cybersecurity incident has forced the temporary closure of Senegal's government office responsible for managing highly sensitive data, including national ID cards, passports, and other biometric records.[4] In February, the Directorate of File Automation (DAF) notified the country's 19.5 million residents that a cyberattack had disrupted operations, leading to a suspension of services. A senior police official said efforts are underway to restore affected systems and maintained that the integrity of citizens' personal data remains intact. The notice came after a ransomware group calling itself Green Blood Group claimed responsibility for breaching the agency and stealing 139 GB of data, including citizen database records, biometric information, and immigration documents.

Norway Says It Was Targeted in Salt Typhoon Cyber Campaign

Norway's domestic security agency has confirmed that the Chinese state-backed espionage campaign known as Salt Typhoon compromised network devices within Norwegian organizations.[5] The disclosure was included in the Norwegian Police Security Service's (PST) 2026 annual threat assessment. Salt Typhoon is the term used by U.S. and allied authorities to describe a Chinese cyber espionage operation that has primarily targeted telecommunications and other critical infrastructure. In its report, PST said the group exploited vulnerable network devices

in Norway. The assessment further noted that Chinese security and intelligence services have enhanced their operational capacity in Norway through cyber operations and human intelligence gathering, stating that "the primary intelligence threat from China is in the cyber domain."[6]

Leak Shows China Rehearsed Cyberattacks Abroad

Leaked technical documents reviewed by media suggest that China may be using a covert training platform to simulate cyberattacks against the critical infrastructure of neighboring countries.[7] For years, Western officials and cybersecurity researchers have accused Beijing of conducting large-scale offensive cyber operations, typically citing intelligence assessments and post-incident technical forensics. The newly leaked materials including source code, training modules, and software tools offer rare documentary evidence of the preparatory work that could underpin such operations before they are carried out.

The leaked cache outlines the platform's engineering design and system architecture, including a dedicated cyber range where operators can simulate and practice hacking operations. It also contains records of incremental software patches, detailed debugging processes, and developer work reports, indicating ongoing refinement and testing.

Korea, Malaysia Police Step Up Cooperation Against Transnational Scams

Police authorities from Korea and Malaysia have signed a memorandum of understanding (MoU) to enhance cooperation in tackling transnational crimes, including online scams.[8] Yoo Jae-seong, acting commissioner general of Korea's National Police Agency, and Malaysia's Inspector-General of Police, Mohd Khalid Ismail, signed the preliminary agreement during talks in Seoul. Yoo also invited Malaysia to join a Korea-led global investigative body launched last October. Officials said Ismail agreed to review measures to strengthen cooperation against emerging forms of cybercrime.

The move comes as Korean police step up efforts to address crimes targeting their nationals in Southeast Asia, following reports of abductions and detention of Koreans in Cambodia linked to criminal syndicates and scam centers. Under the MoU, both sides agreed to promptly share information on transnational criminal activities, including scam operations in Southeast Asia, and to collaborate on joint law enforcement actions such as arrests and the repatriation of fugitives.

Ukraine Says Cyberattacks on Energy Grid Used to Guide Missile Strikes

Ukrainian cybersecurity officials say Russian cyber operations targeting the country's energy infrastructure are increasingly geared toward intelligence gathering to support missile strikes, rather than causing immediate operational disruption.[9] While the number of large-scale cyber incidents against critical infrastructure has declined, the overall threat remains significant, according to Oleksandr Potii, head of Ukraine's State Service of Special Communications and Information Protection. He noted that attackers now appear focused on mapping energy facilities, monitoring repair teams,

and evaluating how quickly systems can recover after strikes, instead of directly triggering power outages.

Home Minister outlines cybersecurity intiatives and enforcement actions

Union Home Minister and Minister of Cooperation, Amit Shah, delivered the keynote address at the National Conference on "Tackling Cyber-Enabled Frauds & Dismantling the ecosystem."[10] In his speech, he emphasised that although multiple Indian agencies are working to combat cybercrime, better alignment and coordination among institutions is essential to achieve meaningful results. He noted that initiatives led by the Central Bureau of Investigation (CBI) and the Indian Cyber Crime Coordination Centre (I4C) aim to bring together different government departments, law enforcement agencies, financial institutions, and regulators to strengthen the country's cybercrime response framework. As a result of this, various enforcement actions taken by authorities included blocking of 1.2 million SIM cards, disabling 300,000 mobile devices, and arresting over 20,000 suspects. Collaboration with banks had helped freeze or recover over ₹8,189 crore from fraudulent transactions.[11]

During the event, he also launched the State Cyber Crime Coordination Centre (S4C) dashboard of the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs.

India File

- Supabase, a widely used developer database platform, has reportedly been blocked in India, one of its key markets.[12] The government directed internet service providers to restrict access to its website, leading to inconsistent availability across networks. According to reports, the blocking order was issued on February 24 under Section 69A of India's Information Technology Act, which grants authorities the power to limit public access to online content. The government has not publicly stated the reason for the move. It remains unclear whether the action is related to cybersecurity concerns, copyright issues, or another matter, as well as how long the restrictions will remain in effect.

- The Indian Computer Emergency Response Team (CERT-In), under the Ministry of Electronics and Information Technology (MeitY), in collaboration with SIA-India, has developed a comprehensive framework and guidelines on Space Cyber Security aimed at securing space communication assets and strengthening the resilience of India's space ecosystem.[13] The document was released at the DefSat Conference & Expo 2026, held in New Delhi from 24–26 February 2026. Advisory in nature, the guidelines are intended to enhance cybersecurity preparedness across the space sector. The framework is designed to support a wide range of stakeholders, including government agencies, satellite service providers, ground station operators, equipment manufacturers, and private space companies. By outlining key cybersecurity principles, recommended safeguards, and clearly defined roles and responsibilities, the guidelines aim to promote resilience, accountability, and proactive risk management throughout the sector.

- The Ministry of Electronics and Information Technology (MeitY) felicitated the winners of the 'Cyber Security Grand Challenge 2.0' (CSGC 2.0), a flagship initiative implemented in collaboration with the Data Security Council of India (DSCI).[14] The programme aims to enhance India's cybersecurity capabilities and build expertise in critical technology domains to support a secure and resilient digital ecosystem. With a combined prize pool of Rs. 6.85 crore, CSGC 2.0 stands among the most significant government-backed cybersecurity innovation challenges in the country. The competition was conducted in four structured stages, featuring progressive evaluation and financial support at each phase.

- The third edition of the Tri-Services Future Warfare Course , held in New Delhi from 2 to 25 February 2026, entered its Cognitive and Cyber Warfare module, which is an essential segment focused on emerging domains of conflict and the evolving character of warfare.[15] The module supports the course's broader objective of equipping officers with a comprehensive understanding of cyber, information, and cognitive warfare, while fostering operational foresight and adaptive thinking. The programme brought together a multidisciplinary group of participants, including officers from the Army, Navy, and Air Force, DRDO scientists, academics, and representatives from the technology and defence industry.

---

[1] Le Monde, Hacker accessed data from 1.2 million bank accounts, French Economy Ministry says, 18 February 2026, https://www.lemonde.fr/en/economy/article/2026/02/18/hacker-accessed-data-from-1-2-million-bank-accounts-french-economy-ministry-says_6750628_19.html

[2] France 24, Hackers steal medical details of 15 million in France, 27 February 2026, https://www.france24.com/en/live-news/20260227-hackers-steal-medical-details-of-15-million-in-france

[3] Inquirer.Net, Italy detects cyber-attacks eyeing Chinese dissidents, 19 February 2026, https://globalnation.inquirer.net/309587/italy-detects-cyber-attacks-eyeing-chinese-dissidents

[4] The Record, Senegal confirms breach of national ID card department after ransomware claims, 10 February 2026, https://therecord.media/senegal-breach-national-id-agency

[5] The Record, Norwegian intelligence discloses country hit by Salt Typhoon campaign, 6 February 2026, https://therecord.media/norawy-intelligence-discloses-salt-typhoon-attacks

[6] Ibid.

[7] The Record, Leaked technical documents show China rehearsing cyberattacks on neighbors' critical infrastructure, 9 February 2026, https://therecord.media/leaked-china-documents-show-testing-cyber-neighbors

[8] The Korea Times, Police authorities of Korea, Malaysia agree to boost cooperation against transnational scams, 4 February 2026, https://www.koreatimes.co.kr/foreignaffairs/20260204/police-authorities-of-korea-malaysia-agree-to-boost-cooperation-against-transnational-scams

[9] The Record, Ukraine says cyberattacks on energy grid now used to guide missile strikes, 23 February 2026, https://therecord.media/ukraine-cyberattacks-guiding-russian-missile-strikes

[10] PIB, Home Minister inaugurated New Cybercrime Branch of CBI and launched State Cyber Crime Coordination Centre (S4C) dashboard of I4C, 10 February 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2226082&reg=3&lang=1

[11] National Informatics Centre. *Conference on "Tackling Cyber-Enabled Frauds & Dismantling the Ecosystem"*. Webcast Services, Government of India, 10 Feb. 2026. https://webcast.gov.in/events/MjkxNQ--

[12] Techcrunch, India disrupts access to popular developer platform Supabase with blocking order, 27 February 2026, https://techcrunch.com/2026/02/27/india-disrupts-access-to-popular-developer-platform-supabase-with-blocking-order/

[13] PIB, India's Space Ecosystem Gets Cyber Shield as SIA-India, CERT-In Release Joint Guidelines, 26 February 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2233122&reg=3&lang=1

[14] PIB, Ministry of Electronics & IT and DSCI felicitated Winners of 'Cyber Security Grand Challenge 2.0' with total prize pool of ₹ 6.85 Cr, 26 February 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2233054&reg=3&lang=1

[15] PIB, Future Warfare Course 3.0 Emphasizes Cognitive and Cyber Domains at Manekshaw Centre, 4 February 2026, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2223362&reg=3&lang=1