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

CYBER *Digest*

August 2025

- France's Naval Group Probes Data Breach
- Cybersecurity crisis hits the aviation sector
- Cyberattack on Brazilian Tech Provider Disrupts Financial Institutions
- Germany Proposes Cyber Dome to Bolster Cybersecurity
- Multiple Arrests in Nepal, Including Chinese Nationals, for Digital Fraud
- Fake Android Money App Targets Bengali-Speaking Users
- India to Deploy City CISOs as Cybercrime Surges
- India File

France's Naval Group Probes Data Breach

France's state-owned defense firm Naval Group is investigating a suspected cyberattack after 1TB of allegedly stolen data was leaked on a hacking forum.[1] Describing the incident as a "reputational attack," the company has filed a formal complaint to safeguard client data. Naval Group, with support from external experts, is working to verify whether the leaked information originated from its systems. Despite the serious claims, the company reports no evidence of a breach or disruption to its operations.

Naval Group was responsible for the production of India's six Scorpene-class submarines (the last of which, the INS Vaghsheer, was delivered to the Indian Navy on January 9, 2025) and builds and maintains various ships and submarines for the French navy, including aircraft carriers and nuclear submarines, while also serving foreign navies such as those of India and Brazil. The incident came to light around July 28, 2025, with the perpetrators claiming to have acquired a substantial amount of confidential information.

The hackers, identifying themselves as "Neferpitou," announced on an underground hacking forum around July 23, 2025, that they had approximately one terabyte (TB) of Naval Group's internal data.[2] This allegedly includes the source code for the combat management and weapon systems integrated into the submarines, as well as source code for French nuclear submarines and frigates, weapon system software, simulation environments, network designs, user manuals, and internal communications. "Neferpitou" provided a 13 gigabyte (GB) "free sample" of the contents and later made 30 GB of the data publicly available online.

In 2016, the company experienced a similar significant breach when over 22,000 pages of classified documents related to India's Scorpene submarines were leaked.[3] At the time, Naval Group (then known as DCNS) was building six Scorpene-class submarines for the Indian Navy in partnership with Mazagon Dock Shipbuilders. DCNS, in response to the 2016 leak, expressed being "stunned" by the information and described it as bearing the hallmarks of "economic warfare" carried out by frustrated competitors.[4] Subsequent investigations indicated that the breach reportedly originated with a disgruntled French subcontractor.[5]

Cybersecurity crisis hits the aviation sector

In July, it was reported that Air Serbia, the state-owned national carrier, postponed issuing staff pay slips after a cyberattack.[6] The airline's IT team immediately treated the incident as a priority, warning employees on 4 July and working to restore systems. Preliminary assessments suggest the breach may have exposed personal data.

In a separate aviation incident, Russia's flag carrier Aeroflot cancelled more than 50 round-trip flights after a debilitating cyberattack claimed by two pro-Ukrainian hacker groups, disrupting travel nationwide.[7] The Kremlin labelled the breach alarming and lawmakers called it a wake-up call, while prosecutors confirmed the hack and opened a criminal investigation.

Cyberattack on Brazilian Tech Provider Disrupts Financial Institutions

Brazil's central bank confirmed that C&M Software, a technology provider supporting financial institutions without their connectivity infrastructure, had suffered a cyberattack.[8] While the bank withheld further details, it ordered C&M to suspend institutional access to its systems. The company acknowledged being directly targeted, with attackers attempting to fraudulently use client credentials to breach its services. An official involved in the investigation noted that C&M Software serves approximately two dozen small financial institutions, potentially amplifying the impact of the cyberattack.

Germany Proposes Cyber Dome to Bolster Cybersecurity

In response to the recent military and cyber escalation between Israel and Iran, Germany plans to deepen its cybersecurity cooperation with Israel and establish a joint cyber research center.[9] According to reports, German Interior Minister Alexander Dobrindt unveiled the initiative during a visit to Israel. Dubbed the Cyber Dome, the plan includes the creation of a German-Israeli cyber research center, enhanced collaboration between Israel's Mossad and Germany's BND intelligence agency, strengthened cyber and anti-drone defenses, and the development of a nationwide emergency alert and civil shelter system modeled after Israel's.

Multiple Arrests in Nepal, Including Chinese Nationals, for Digital Fraud

The Central Investigation Bureau (CIB) of Nepal Police has arrested 52 individuals, including six Chinese nationals, for allegedly operating an online scam involving a fake dating app and cryptocurrency trading under the guise of a registered tech company.[10]

According to a CIB press release, the group had set up operations in two rented houses and registered a front company named Social Software Development Company Pvt Ltd to mask their illicit activities. Investigators revealed that the suspects were running a fake call center and using a dating app called METOO Dating App to lure young Nepali women and carry out fraudulent online transactions.

Fake Android Money App Targets Bengali-Speaking Users

A cybersecurity firm has uncovered an active Android malware campaign specifically targeting Bengali-speaking users, primarily Bangladeshi expatriates. Disguised as trusted financial apps like TapTap Send and AlimaPay, the malicious apps are spread via phishing websites and are designed to steal users' personal and financial data.[11]

The campaign remains highly active, with a functioning command-and-control (C2) server linked to multiple evolving domains. While the techniques used are not new, the attackers' cultural targeting and sustained efforts highlight how cybercriminals adapt to exploit specific communities. Bangladeshi nationals living abroad, especially in countries such as Saudi Arabia, the UAE, Malaysia, and the UK- heavily rely on mobile money services like bKash, TapTap Send, and AlimaPay for remittances and identity verification, making them prime targets for such scams.

India to Deploy City CISOs as Cybercrime Surges

The Union Ministry of Home Affairs (MHA) has officially confirmed that Indian citizens lost over Rs. 22,845.73 crore to cyber fraud in 2024, a staggering 206% increase from Rs. 7,465.18 crore in 2023.[12] The data highlights the alarming rise in cybercrime-related financial losses across the country.

During a two-day meeting in Delhi, Parliamentary Standing Committee on Home Affairs focused on the implications, security challenges, and prevention strategies related to cybercrime. [13] The session featured detailed discussions on strengthening cybercrime prevention measures. Representatives from the Ministry of External Affairs, Ministry of Corporate Affairs, Financial Intelligence Unit-India (FIU-IND), Central Bureau of Investigation (CBI), National Investigation Agency (NIA), and both public and private sector banks presented their perspectives on combating cybercrime and enhancing digital security frameworks.

The Indian Computer Emergency Response Team (CERT-In) has also issued new Comprehensive Cyber Security Audit Policy Guidelines to standardize and strengthen cybersecurity audits across public and private sectors.[14] The guidelines provide a detailed framework covering the full audit lifecycle, from planning and scoping to execution, reporting, and follow-up. By focusing on critical elements such as asset management, risk assessment, vulnerability analysis, and governance structures, the policy aims to promote greater discipline and maturity in how organizations secure their IT environments.

The government has also introduced new regulations for defence companies operating in India, emphasizing bolstering cybersecurity and strengthening physical security at manufacturing facilities.[15] The new Security Manual for Licensed Defence Industries mandates firms to invest in robust information and perimeter security measures, conduct regular emergency response drills, and work closely with law enforcement agencies to verify employee backgrounds. The move aims to prevent data breaches and enhance security within the defence manufacturing sector.

Amid rising digital threats, the Union Home Ministry has urged every Indian city to appoint a Chief Information Security Officer (CISO) to safeguard critical systems and citizen data.[16] With the rapid expansion of smart cities, the initiative aims to build in-house cyber resilience beyond reliance on private consultants and third-party vendors. During a high-level meeting on cybersecurity preparedness in New Delhi, Union Home Secretary Govind Mohan emphasized the urgent need for dedicated CISOs in each city to defend local digital infrastructure and data from evolving cyber threats.

India File

- Indian cryptocurrency exchange CoinDCX suffered a $44 million loss in a suspected sophisticated server breach.[17] One of its employees has been arrested in connection with the hack. The stolen cryptocurrency was routed through multiple wallets to evade detection, complicating efforts to trace it.[18] Police later uncovered evidence suggesting insider involvement and arrested a CoinDCX employee during the investigation.

- The Indian Council of Agricultural Research (ICAR), the country's top agricultural research body, suffered a security breach earlier this year, resulting in the loss of crucial data spanning recruitment and research projects.[19] ICAR formed a six-member committee this month to review the non-functionality of its Data Centre (DC) and Disaster Recovery Centre (DRC) and recommend measures to strengthen data security and prevent future breaches.

- Max Financial Services reported that its insurance arm, Axis Max Life Insurance, received a message from an anonymous source alleging unauthorized access to customer data.[20] The company stated in a stock exchange filing that Axis Max Life promptly launched an information security assessment and data log analysis. A detailed investigation is underway, with cybersecurity experts assisting in identifying the root cause and implementing corrective measures.

---

[1] Bleeping Computer, "France's warship builder Naval Group investigates 1TB data breach", 28 July 2025, https://www.bleepingcomputer.com/news/security/frances-warship-builder-naval-group-investigates-1tb-data-breach/

[2] Graham Cluley, "French Submarine Secrets Surface after Cyber Attack." *Bitdefender HotforSecurity*, 28 July 2025, www.bitdefender.com/en-us/blog/hotforsecurity/french-submarine-secrets-surface-after-cyber-attack

[3] BBC News "India Investigating French Submarine Company Data Leak." 24 Aug 2016, www.bbc.com/news/business-37171856.

[4] India Today, "India Shelves Plan to Expand French Submarine Order after Scorpene Data Breach.", 2 September. 2016, www.indiatoday.in/india/delhi/story/india-shelves-plan-to-expand-french-submarine-order-after-scorpene-data-breach-338899-2016-09-02

[5] "Submarine Data Leak Roils Three Governments." Defense News, 27 Aug 2016, www.defensenews.com/naval/2016/08/26/submarine-data-leak-roils-three-governments

[6] The Register, "Turbulence at Air Serbia, the latest airline under cyber siege", 16 July 2025, https://www.theregister.com/2025/07/16/air_serbia_cyberattack/

[7] Reuters, "Pro-Ukrainian hackers claim massive cyberattack on Russia's Aeroflot", 28 July 2025, https://www.reuters.com/en/pro-ukrainian-hackers-claim-massive-cyberattack-russias-aeroflot-2025-07-28/

[8] The Hindu, "Cyberattack on Brazil tech provider affects reserve accounts of some financial institutions", 3 July 2025,https://www.thehindu.com/sci-tech/technology/cyberattack-on-brazil-tech-provider-affects-reserve-accounts-of-some-financial-institutions/article69766899.ece

[9] The Record, "Germany seeks deeper partnership with Israel on cybersecurity", 2 July 2025, https://therecord.media/germany-israel-deepen-cyber-cooperation

[10] The Kathmandu Post, "52 people, including six Chinese nationals, arrested for online dating scam and illegal crypto trade", 2 July 2025, https://kathmandupost.com/national/2025/07/02/52-people-including-six-chinese-nationals-arrested-for-online-dating-scam-and-illegal-crypto-trade

[11] McAfee, "Fake Android Money Transfer App Targeting Bengali-Speaking Users", 14 July 2025, https://www.mcafee.com/blogs/other-blogs/mcafee-labs/fake-android-money-transfer-app-targeting-bengali-speaking-users/

[12] The New Indian Express, "Indian citizens lost over Rs 22,845 crore to online fraudsters in 2024: MHA in Lok Sabha", 22 July 2025, https://www.newindianexpress.com/nation/2025/Jul/22/indian-citizens-lost-over-rs-22845-crore-to-online-fraudsters-in-2024-mha-in-lok-sabha

[13] The Statesman, "Parliamentary panel discusses measures to combat cyber fraud", 4 July 2025, https://www.thestatesman.com/india/parliamentary-panel-discusses-measures-to-combat-cyber-fraud-1503453503.html

[14] The 420, "New CERT-In Audit Guidelines Aim to Fix India's 'Checkbox' Cybersecurity Culture — Here's How", 25 July 2025, https://the420.in/cert-in-cybersecurity-audit-guidelines-2025-sanjay-bahl-compliance-to-resilience-policy-framework/

[15] The Economic Times, "New security code kicks in for defence companies in India", 24 July 2025, https://economictimes.indiatimes.com/news/defence/new-security-code-kicks-in-for-defence-companies-in-india/articleshow/122866419.cms?from=mdr

[16] The 420, "Union Home Secretary Mandates Appointment of Chief Information Security Officer (CISO) in Every City", 19 July 2025, https://the420.in/smart-cities-cybersecurity-india-ciso-mandate/

[17] Cointelegraph, "Crypto hacks top $142M in July, with CoinDCX leading losses", 1 August 2025, https://cointelegraph.com/news/crypto-hacks-july-142-million-coindcx-leads-losses

[18] Deepak Bopanna, "Hackers Steal Rs 380 Crore In Cryptocurrency From CoinDCX, Employee Arrested", NDTV, 30 July 2025

[19] The Indian Express, "Data breach at ICAR hits key recruitment, agri research projects", 25 July 2025, https://indianexpress.com/article/india/data-breach-at-icar-hits-key-recruitment-agri-research-projects-10147925/

[20] TechCrunch, "India's Max Financial says hacker accessed customer data from its insurance unit", 2 July 2025, https://techcrunch.com/2025/07/02/indias-max-financial-says-hacker-accessed-customer-data-from-its-insurance-unit/