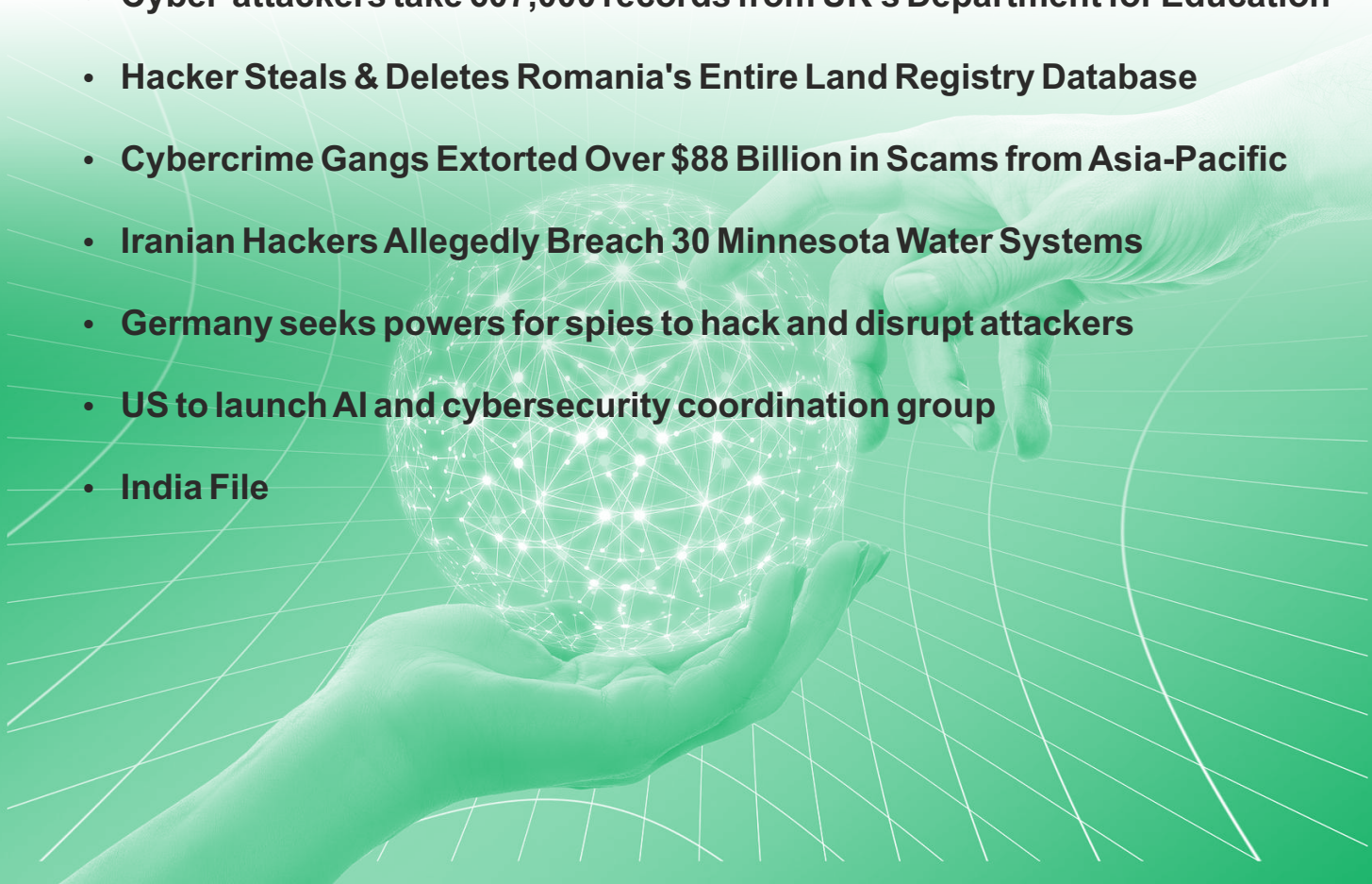
MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR
DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

CYBER *Digest*

August 2026

- Data breach at India's largest nuclear power plant in Kudankulam
- New cars in EU to include a camera aimed at the driver's face
- Cyber-attackers take 607,000 records from UK's Department for Education
- Hacker Steals & Deletes Romania's Entire Land Registry Database
- Cybercrime Gangs Extorted Over $88 Billion in Scams from Asia-Pacific
- Iranian Hackers Allegedly Breach 30 Minnesota Water Systems
- Germany seeks powers for spies to hack and disrupt attackers
- US to launch AI and cybersecurity coordination group
- India File



Data breach at India's largest nuclear power plant in Kudankulam

A ransomware group, World Leaks, published nearly 19,000 files (14.3 GB) allegedly linked to the Kudankulam Nuclear Power Plant in India on the dark web[1]. It reportedly obtained them from one of the plant contractors – Anil Ambani's Reliance group, following a partial breach of data hosted on a third party server (Yotta). The leaked files, dated from 2016 to 2025, include blueprints of support facilities, supplier information, inspection records, and insurance documents. While the Nuclear Power Corporation of India stated that no nuclear safety or security systems were compromised, CERT-In (the Indian Computer Emergency Response Team) is investigating the incident. Cybersecurity experts warned that such information could help adversaries map critical infrastructure and supply chains, highlighting persistent cybersecurity vulnerabilities in India's critical infrastructure.

New cars in EU to include a camera aimed at the driver's face

The European Union has implemented new vehicle safety regulations requiring all newly manufactured and sold cars to be equipped with Advanced Driver Distraction Warning (ADDW) systems, which use infrared cameras to monitor drivers' head position and eye movements to detect distraction[2]. Similar requirements are scheduled to take effect in the United States next year. The regulations stipulate that biometric data must not be collected and that all data processing should remain within the vehicle. However, privacy advocates have raised concerns over enforcement, citing the automotive industry's poor record on data privacy. Reports that some manufacturers may process driver data on external servers have further intensified concerns regarding compliance and potential misuse of driver data.

Cyber-attackers take 607,000 records from UK's Department for Education

The UK's Department for Education (DfE) confirmed a cyberattack in which hackers accessed approximately 607,000 records containing customer service contact information, including telephone numbers and email addresses of individuals and organisations[3]. The department stated that no financial or other sensitive personal data was compromised and assessed the risk to affected individuals as low. The breach impacted the Turing Scheme portal and the DfE online help desk. The DfE is working with the National Cyber Security Centre, the National Crime Agency, and the Information Commissioner's Office to understand the circumstances and impact of the cyberattack.

Hacker Steals & Deletes Romania's Entire Land Registry Database

Romania's National Agency for Cadastre and Real Estate Advertising (ANCPI) suffered a major cyberattack in which a hacker allegedly erased the country's land registry database after a failed extortion attempt[4]. The breach disrupted Romania's real estate sector, leaving land registry services, official websites, applications, and email systems offline for over a week, preventing property transactions and ownership verification. The attacker reportedly gained access using valid credentials, mapped internal systems, and wiped all the backups. Authorities have

begun rebuilding the agency's network from scratch and are restoring services using offline backups.

Cybercrime Gangs Extorted Over $88 Billion in Scams from Asia-Pacific

A UNODC report warned that cyber-enabled scam syndicates in Southeast Asia continue to outpace law enforcement, defrauding victims across the Asia-Pacific of an estimated US$88.3-114.1 billion in 2025[5]. The report touched upon the evolution of criminal activities in Southeast Asia, a region known for being an epicentre for cyber fraud by mostly Chinese-origin syndicates, into highly organised, franchise-like operations spanning money laundering, human trafficking, migrant smuggling, and data trading. Despite regional crackdowns, syndicates relocated to jurisdictions with weaker governance, including East Timor, Pacific Island states, and parts of Africa. The report identified corruption as a key enabler and warned that criminals were increasingly leveraging generative and agentic AI to automate victim targeting, social engineering, cryptocurrency theft, and other cyber-enabled crimes.

Iranian Hackers Allegedly Breach 30 Minnesota Water Systems

A coordinated cyberattack targeted more than 30 community water and wastewater systems in Minnesota, United States on 26-27 July, disrupting operational technology and prompting a state-wide response, even involving the FBI[6]. One water treatment plant was temporarily shut down, while several utilities disconnected automated equipment and shifted to manual operations. Security researchers assess the attack bears the hallmarks of "CyberAv3ngers", an Iranian state-linked hacking group. The incident followed a recent U.S. advisory warning of the group's expanded targeting of industrial control systems and exploitation of an unpatched critical vulnerability. Drinking water quality was not impacted, and investigations remain ongoing.

Germany seeks powers for spies to hack and disrupt attackers

Germany is proposing a major overhaul of its intelligence laws to grant spy agencies offensive cyber powers in response to growing cyber and hybrid threats, particularly from Russia[7]. The draft legislation would allow intelligence services to hack attackers' systems, delete or copy data, disrupt hostile cyber infrastructure, and conduct targeted disinformation campaigns under strict legal thresholds. It also introduces new surveillance powers, expands the use of state spyware, and authorises secret data disclosure orders for telecom, digital, transport, and financial firms. To strengthen accountability, the reforms establish an Independent Control Council to oversee and approve the most intrusive intelligence operations.

US to launch AI and cybersecurity coordination group

The United States plans to establish a formal coordination mechanism between leading AI developers and critical infrastructure operators to share information on cybersecurity vulnerabilities identified by advanced AI systems[8]. The initiative aims to prevent malicious exploitation of software vulnerabilities affecting essential sectors such as finance, healthcare, and energy,

while avoiding duplication of defensive efforts. The collaboration includes developers of both proprietary and open-source AI models and is supported by the Treasury Department, National Cyber Director's Office, Department of Defense, and National Security Agency.

India File

- Bank of Baroda is investigating claims that a threat actor breached its systems and leaked approximately 1 TB of data on the dark web, allegedly exposing customer and internal records, including account details, Aadhaar numbers, loan information, Net Banking data, and branch documents[9]. The bank clarified in a statement that the incident resulted from the compromise of an employee's email account, with no breach of its core banking systems. The statement also said that the bank had launched containment measures and a forensic investigation in coordination with relevant authorities. While independent researchers verified samples of the leaked data, the attack has been tentatively linked to a threat actor operating under the name "leak-king-F".

- At the eighth India-Japan Defence Policy Dialogue held in Tokyo, both countries agreed to deepen cooperation across defence industrial collaboration, technological innovation, cyber security, space, maritime technology, and other emerging domains[10]. The two sides reviewed progress in bilateral defence ties, including military exchanges, joint exercises, capacity building, and defence equipment cooperation, while reaffirming their commitment to the India-Japan Special Strategic and Global Partnership.

- The Government of India directed Apple and Google to remove the "BAT-BMS" battery management application from their app stores after it was misused to remotely disable e-rickshaws as part of a viral prank challenge[11]. The app, originally designed to manage and diagnose compatible lithium batteries via Bluetooth, was exploited to shut down vehicles whose batteries lacked password protection, causing traffic disruptions and financial losses for drivers. Although the application has been removed from the Indian Apple App Store and Google Play Store, it remains available through third-party platforms and alternate store regions.

- A ransomware attack on Tata Electronics, claimed by the World Leaks group, has reportedly exposed sensitive Apple supply chain data, including component lists, supplier mappings, and photographs of unreleased iPhone 18 Pro models[12]. The leaked files allegedly reveal detailed information on hardware components, suppliers, and internal testing, potentially exposing Apple's supply chain vulnerabilities and commercial relationships. Apple is investigating the breach alongside Tata, which has restricted access to sensitive systems and initiated a forensic audit.

- The Securities and Exchange Board of India (SEBI) issued an advisory - warning regulated entities and listed companies about the growing threat of "Boss Scam" fraud, wherein attackers impersonate CEOs or senior executives to deceive finance personnel into transferring funds[13]. SEBI highlighted tactics including fake emails, WhatsApp messages, AI-enabled voice cloning, deepfake video calls, and malware-laden

ZIP files that hijack WhatsApp Web sessions or compromise devices. The advisory, issued following an alert from the Indian Cyber Crime Coordination Centre (I4C), urges organisations to independently verify payment requests, avoid acting solely on digital instructions, close active WhatsApp Web sessions, and refrain from opening unverified files.

- Cert-In conducted an online training program on the topic "From Code to Cloud: Secure APIs with a Robust SDLC" on July 14, 2026[14]. This was undertaken exclusively for officials handling application development, security of applications & IT Security from various IT/ITeS and BFSI organizations. The training aimed to provide insights on API security and highlight the importance of Secure Software Development Life Cycle (SSDLC).

[1] Files relating to India's largest nuclear power plant Kudankulam exposed in data breach, July 15 2026, https://www.reuters.com/world/india/files-relating-indias-largest-nuclear-power-plant-kudankulam-exposed-data-breach-2026-07-15/

[2] New EU Car Safety Rules Take Effect 7 July: How Your Car Could Monitor You, July 6 2026, https://www.inkl.com/glance/news/new-eu-car-safety-rules-take-effect-7-july-how-your-car-could-monitor-you?first_login=true&section=personalized

[3] Cyber-attackers take 607,000 records from Department for Education, July 29 2026, https://www.bbc.com/news/articles/cq6dmgrp21po

[4] A Hacker Stole Romania's Entire Land Registry Database — Then Deleted It, July 22 2026, https://www.iansresearch.com/resources/all-blogs/post/security-blog/2026/07/22/a-hacker-stole-romania-s-entire-land-registry-database---then-deleted-it

[5] Cybercrime Gangs Extorted Over $88 Billion In Scams From Asia-Pacific: Report, July 21 2026, https://www.ndtv.com/world-news/un-reports-88-billion-cybercrime-losses-in-asia-pacific-in-2025-11799359

[6] Iranian Hackers Exploited Unpatchable PLC Flaw to Breach 30 Minnesota Water Systems, July 29 2026, https://www.techtimes.com/articles/322059/20260729/iranian-hackers-exploited-unpatchable-plc-flaw-breach-30-minnesota-water-systems.htm

[7] Germany seeks powers for spies to hack and disrupt attackers, July 2 2026, https://www.reuters.com/technology/germany-seeks-powers-spies-hack-disrupt-attackers-2026-07-02

[8] US to launch AI and cybersecurity coordination group, White House says July 15 2026, https://www.reuters.com/technology/us-launch-ai-cybersecurity-coordination-group-white-house-says-2026-07-14

[9] India's Bank of Baroda confirms cyber incident after hackers claim data theft, July 28 2026, https://therecord.media/india-bank-of-baroda-reports-cybersecurity-incident

[10] India, Japan review defence ties, prepare ground for 2+2 dialogue later this year, July 14 2026, https://www.thehindu.com/news/international/india-japan-hold-key-dialogue-to-boost-ties-in-defence-industrial-collaboration-cyber-security/article71216991.ece

[11] Viral App BAT-BMS Under Scanner After Delhi E-Rickshaws Disabled Remotely, Drivers Left Helpless, July 3 2026, https://www.timesnownews.com/delhi/bat-bms-app-delhi-e-rickshaw-drivers-stranded-bluetooth-prank-probe-article-154893620

[12] Apple iPhone 18 Pro supplier list, parts and photos exposed in Tata data leak, https://www.msn.com/en-in/money/technology/apple-iphone-18-pro-supplier-list-parts-and-photos-exposed-in-tata-data-leak/ar-AA26PUQo?ocid=sapphireappshare

[13] SEBI flags 'Boss Scam' that targets C-suite officials, July 17 2026, https://www.thehindu.com/business/markets/sebi-flags-boss-scam-that-targets-c-suite-officials/article71234552.ece/amp/

[14] Workshop on "From Code to Cloud: Secure APIs with a Robust SDLC", July 14 2026, https://www.cert-in.org.in/s2cMainServlet?pageid=PRSTNVIEW012&year=2026