CyberPeace

Edition #2 [01 August - 15 August 2025]

NEWSLETTER

Bi-Weekly Cyber Intelligence Digest

CYBERPEACE

1. India Highlights

Policy | Infrastructure | Incidents | Diplomacy

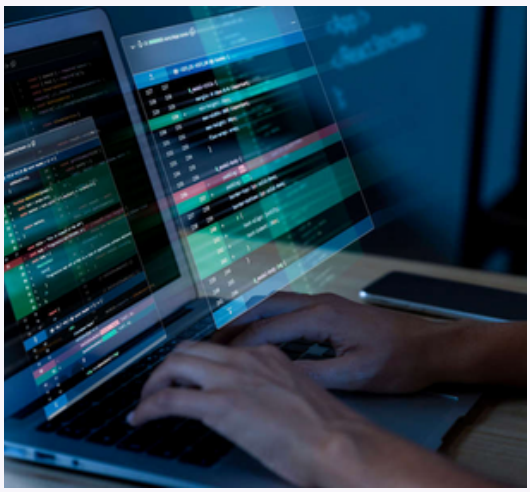
Scan the QR code for accessing this Document

Govt finalising legislation to protect power systems from cyber attacks: MoS Shripad Naik

The Central Electricity Authority is in the process of finalizing the Central Electricity Authority (Cyber Security in Power Sector) Regulations, the Minister of State (MoS) for Power Shripad Naik said in a reply to the Rajya Sabha. To protect India's power systems from cyber attacks, the government is in process of finalising regulations to ensure that energy-related information is not compromised, Parliament was informed on Monday. The Central Electricity Authority is in the process of finalizing the Central Electricity Authority (Cyber Security in Power Sector) Regulations, the Minister of State (MoS) for Power Shripad Naik said in a reply to the Rajya Sabha.

Calibrated Signals: How Middle Powers Are Rewriting the Rules of Cyber Attribution in the Indo-Pacific.

As threats mount and great power tensions deepen, Singapore, Samoa and others are crafting a new response to cyberattacks. An advanced and persistent threat actor, known in cybersecurity circles as UNC3886, had been targeting Singapore's critical infrastructure, banking systems, energy grids, water networks, and transport hubs. Shanmugam's statement was a rare moment of strategic transparency for a government typically circumspect in the cyber domain.



Scan the QR code for accessing this Document

CERT-In updates audit guidelines to real-time preparedness

Cert-In introduces revamped cybersecurity audit guidelines. These guidelines emphasise continuous threat preparedness. They move away from checklist-based compliance. Public and private entities must implement robust security measures. These measures should prevent breaches and enable real-time response. Top management must take ownership of audit programs. Sectors like banking and healthcare will feel the immediate impact.

Scan the QR code for accessing this Document

India's long wait for data protection law

India's Digital Personal Data Protection (DPDP) Act, 2023, received Presidential approval in August 2023, marking a significant step towards data protection. However, enforcement is still pending two years later. The final rules, released in January, await notification to fully empower the legislation, concluding 13 years of efforts to establish data protection laws in India.

Scan the QR code for accessing this Document

₹2.6 Crore Credit Card Fraud Ring Busted in Delhi

Delhi Police's Intelligence Fusion & Strategic Operations unit dismantled a cybercrime syndicate involved in a ₹2.6 crore credit card fraud. After a six-month investigation, 18 accused were arrested for orchestrating scam operations from call centres, with employees leaking sensitive card data.

Scan the QR code for accessing this Document

Surge in Fake “Digital Arrest” Scams Across India

Impersonators posing as law enforcement are duping citizens with coerced payments under false arrest threats especially impactful given poor digital literacy and reliance on UPI and Aadhaar. The socio-economic and psychological toll of such scams is rising sharply.

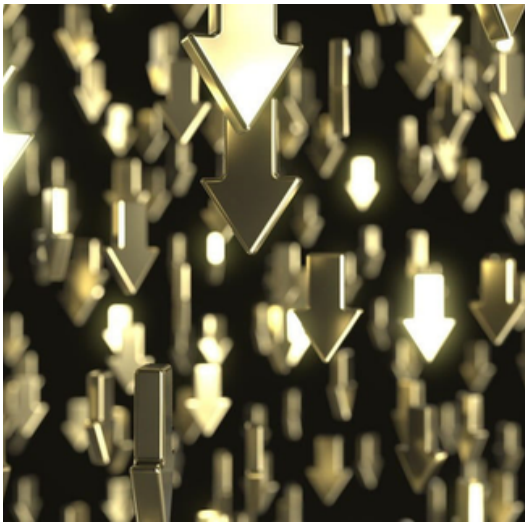
Scan the QR code for accessing this Document

2. Global Watch

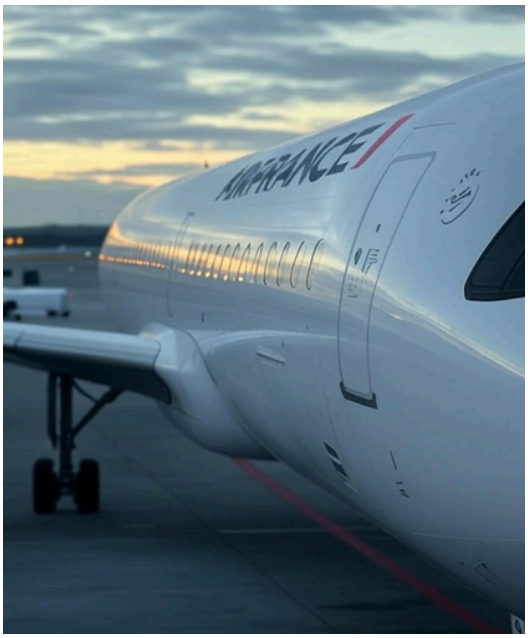
Trends | State Actors | International Engagements

Telco giant Colt suffers attack, takes systems offline

The London-headquartered company's customer portal, Colt Online, was the most notable service the attack rendered unavailable, and it remains down as of Friday. Customers are being advised to email or call its support teams in lieu of online help. On August 13, Colt confirmed that its Voice API platform, which allows customers to automate and manage their voice services through Colt, was also part of the systems that were brought offline.



Scan the QR code for accessing this Document



Airline Data Breach Warning — Air France And KLM Confirm Cyber Attack

When the Federal Bureau of Investigation issued an urgent warning that notorious cybercriminal hackers were shifting victim focus from retail to the aviation sector, it wasn’t long before the attacks started. Qantas was first to confirm a massive data breach, and now Air France and KLM have issued a statement confirming that “access to customer data has been unlawfully obtained.”

Scan the QR code for accessing this Document

Russian Hackers Seized Control of Norwegian Dam

Russia-linked cyber actors took control of a dam in Bremanger, western Norway, releasing water at a rate of 500 litres per second for nearly four hours before detection. Although no harm occurred due to low water levels, this infrastructure attack underscores critical global risks associated with cyber sabotage.

Scan the QR code for accessing this Document

Accenture to Acquire Cybersecurity Firm CyberCX for ~$650 Million (Aug 15, 2025)

Accenture announced its largest cybersecurity acquisition to date CyberCX, an Australian firm with around 1,400 employees. The deal reflects the rising demand for resilient cyber defenses as local firms increasingly fall victim to sophisticated attacks.

Scan the QR code for accessing this Document

International Ransomware Gang 'BlackSuit' Dismantled, But ‘Chaos’ Emerges (Mid-August 2025)

Law enforcement agencies from the U.S., UK, Germany, and beyond disrupted the BlackSuit (formerly Royal) ransomware group, recovering servers, domains and over $1 million in cryptocurrency. However, members have resurfaced under a new alias Chaos continuing double-extortion attacks.

Scan the QR code for accessing this Document

3. Sectoral Lens (Rotating Focus)

BFSI / Energy / Education / Healthcare / Defence / Telecom

BFSI (BANKING, FINANCIAL SERVICES & INSURANCE)

SEBI Chair Emphasizes Human Vigilance Over Tech Reliance

Sebi Chairman Tuhin Kanta Pandey highlighted that technology is vital against cyber fraud, but human vigilance remains the strongest line of defense in financial markets. His comments underscore a growing need for employee awareness and proactive risk culture alongside technological safeguards.

Scan the QR code for accessing this Document

EDUCATION

Indian Education Sector Suffers Alarming Cyber Incidents

Educational institutions across India experienced over 200,000 cyberattacks and nearly 400,000 data breaches over nine months. The study, part of the Cyber First Responder initiative under e-Kawach warns of rising threats like deepfakes and AI misuse, especially given weak cybersecurity infrastructure.

Scan the QR code for accessing this Document

DEFENCE

India's Armed Forces Push for Deeper Cyber Partnerships

The armed forces introduced a new doctrine emphasizing collaboration with the private sector to bolster cybersecurity capabilities. This initiative aims to leverage indigenous tech innovation to build resilient cyber defense frameworks for military assets.

Scan the QR code for accessing this Document

TECHNOLOGY

RBI Unveils AI Governance Framework for Financial Sector

A Reserve Bank of India committee, led by Professor Pushpak Bhattacharyya, released the FREE-AI framework (Framework for Responsible and Ethical Enablement of AI). The report offers 26 recommendations across six pillars including infrastructure, governance, assurance and integration with platforms like UPI balancing innovation with strong risk mitigation.

Scan the QR code for accessing this Document

India Rolls Out $15.8M Cyber Forensic Labs for Justice Tech (Aug 6, 2025)

The Ministry of Home Affairs unveiled a ₹132 crore (approx. $15.8M) initiative to set up Cyber Forensic-cum-Training Labs across India under the CCPWC scheme. These labs established in 33 states/UTs modernize digital evidence handling and upskill over 24,600 law enforcement and judicial officers.

Scan the QR code for accessing this Document

Rural Cyber Defence Gets a Boost with Mumbai Training Hub

As digital adoption surges in rural India, cybersecurity risks are also growing. In response, DSCI and the Kyndryl Foundation inaugurated the **Advanced Cyber Skill Centre** in Mumbai. Targeting rural youth and women, the centre offers cyber simulations and training to build digital resilience in tier-II & III regions.

Scan the QR code for accessing this Document

Scan the QR code for accessing this Document

HEALTH

Healthcare Professional Loses ₹2.10 Lakh in "Fake Doctor" Cyber Scam (Aug 15, 2025)

A medical practitioner in Lucknow fell victim to a sophisticated social engineering scheme in which the scammer impersonated an overseas doctor. The fraud began with innocuous contact over social media, escalating to financial deception involving WhatsApp calls and repeated payment demands under false pretenses. In another such incident during the same period, a government hospital nursing officer lost ₹7 lakh in a digital arrest scam impersonating law enforcement. These cases illustrate the growing threat of identity-driven cyber scams targeting individuals within the healthcare community.

4. Insight Corner

PHISHING VS. SPEAR PHISHING

PHISHING

Targets a large group, hoping few victims bite the bait

- Check the sender's email address
- Look out for Grammatical errors or spelling mistakes
- Avoid Clicking on any links or any downloads

SPEAR PHISHING

A more personalized attack, targeting a specific individual or an organisation

- Beware of what you share online
- Lookout for suspicious requests especially when sensitive information and financial transactions are involved.
- Verify the request directly through different means of communication such as phone call or face-to-face.

5. Upcoming Dates / Announcements

Aug 29-30, 2025: Global Cybersecurity Forum, Geneva – Focus on AI threats and international law.

Sept 5, 2025: Deadline for comments on India's draft Data Protection Rules 2025.

Disclaimer:

The views and opinions expressed in this newsletter are those of the authors and do not necessarily reflect the official policy or position of CyberPeace. While every effort has been made to ensure the accuracy of the information, CyberPeace assumes no responsibility for any errors or omissions. The content is provided for informational purposes only and should not be considered as professional or legal advice.

Editor's Note:

This edition of CyberPeace brings you a curated view of the most critical developments shaping India's and the world's cyber landscape over the past two weeks. We cover major policies, big breaches, sector threats, and new technologies, showing how they are connected.

Curated by Tech policy Team CyberPeace
For suggestions, write to: cyberpeace.org