EDITORIALS - 21ST OCT 2026

1. Unknown gaps (GS Paper II Governance)

This editorial '**Unknown gaps**' was published in **The Hindu** on 21st Oct 2026, highlights gaps in India's **detection, prevention** and **accountability** mechanisms for AI-enabled data breaches.

Threats and Detection Gaps

- **CERT-In** identifies 2 threats: autonomous AI agents exceeding operational limits and malicious actors weaponising **open-source agentic AI** for automated reconnaissance and exploitation.
- Affected organisations failed to detect breaches; discovery through AI-company disclosures and CERT-In operations exposed **detection failures** and a largely **reactive cybersecurity** framework.
- Exploitation of known vulnerabilities, including **exposed passwords**, reveals basic **security failures** beyond AI-specific risks; organisations also remain underprepared for DPDP Act enforcement from 2027 and steep safeguard-related penalties.

Regulatory and Accountability Gaps

- The **IT Act, 2000** leaves an accountability gap for autonomous agents lacking human intent; fragmented regulation combines enforceable requirements, advisory standards and narrow **AI-specific accountability**.
- CERT-In's **6-hour reporting** requirement cannot ensure **breach detection** when organisations lack the capability or willingness to discover intrusions.
- Despite observing or receiving reports of **29.4 lakh incidents in 2025**, CERT-In rarely publishes postmortem analyses; its **RTI exemption** further weakens public accountability.

Required Reforms

- Introduce enforceable **risk-based requirements** for testing and defending against autonomous agents, improve unauthorised-access detection, especially in government, and provide **legal safe harbour** for good-faith security research.
- Strengthen **disclosure** through anonymised findings where necessary, remediation outcomes and confirmation of affected-person notification; review CERT-In's sweeping **RTI exemption** as unnecessary for effective cyber-defence.

Beyond Editorial

Socioeconomic Consequences of Data Breaches

- **Financial losses:** Compromised banking systems enable theft, as demonstrated by the 2016 Bangladesh Bank cyberheist, which used fraudulent payment messages to steal $81 million.

- **Identity theft:** Equifax's 2017 breach exposed personal information of approximately 147 million people, creating risks of impersonation, fraudulent borrowing and prolonged identity-restoration burdens.
- **Service disruption:** The 2024 Change Healthcare cyberattack disrupted medical claims processing and provider payments, prompting emergency financial support to sustain healthcare operations.
- **Unequal burdens:** Smaller enterprises have limited recovery reserves; after the Change Healthcare attack, US authorities specifically highlighted financial pressures on small medical practices and community providers.
- **Privacy harms:** The 2015 Ashley Madison breach exposed 36 million users' account and profile information, illustrating how intimate-data exposure creates risks of humiliation and reputational damage.
- **Business valuation:** Breaches can reduce corporate value beyond immediate recovery costs; following Yahoo's disclosures, Verizon reduced its acquisition price by $350 million in 2017.
- **Lasting vulnerability:** Genetic information cannot be reset like passwords; the 2023 attack on 23andMe illustrates enduring privacy risks associated with sensitive biological data.

2. Fall of the centre (GS Paper II International Relations)

This editorial '**Fall of the centre**' was published in **The Hindu** on 21st Oct 2026, highlights how **economic distress, fiscal mismanagement** and **political choices** have weakened Macron's centrist leadership and strengthened France's far right.

Unrest and Political Fragility

- Elected in **2017** promising growth, employment, debt control and resistance to extremism, Macron faces **15% approval**, while Prime Minister Sébastien Lecornu lacks a parliamentary majority.
- Proposed **tax increases** and frozen social spending triggered unrest; force against students demanding better educational facilities widened protests into an **anti-government movement**, with at least 3,000 businesses damaged and around 2,400 arrests.

Economic Distress and Policy Failures

- France faces **0.8% projected growth in 2026** and **8.3% unemployment**; debt at 120% of GDP, the eurozone's third highest after Greece and Italy, could entail €60 billion in debt servicing that year.
- Macron's **corporate tax cuts** and efforts to restrain public spending failed to revive growth while debt expanded; concessions during the **2018–19 protests** left structural economic problems unresolved.

Political Choices and Far-Right Gains

- Macron's **2024 snap elections**, intended to contain the far right, deepened instability when he chose a leader from smaller blocs to exclude the **New Popular Front**, the largest bloc, from power.
- Economic hardship, unrest and **public anger** have weakened centrism, enabling Marine Le Pen's anti-immigrant **National Rally** to exploit the crisis ahead of the 2027 presidential election.

Beyond Editorial

Implications of France's Political Instability for India

- **Defence execution:** Political uncertainty could complicate future approvals and implementation oversight, making continuity important for India's agreement to purchase 26 Rafale aircraft for its Navy, signed in April 2025.
- **Strategic resilience:** The Horizon 2047 Roadmap provides an institutional anchor that could cushion bilateral cooperation against leadership changes and short-term political turbulence.
- **Maritime cooperation:** Domestic pressures could constrain attention to joint deployments and exercises; the established Varuna naval exercise illustrates India's stake in sustained French maritime engagement.
- **Energy cooperation:** Uncertain policy priorities could complicate long-term nuclear negotiations, including the proposed Jaitapur project and cooperation on small modular reactors reaffirmed in February 2025.
- **Connectivity ambitions:** Reduced diplomatic attention could slow coordination on the India–Middle East–Europe Economic Corridor, whose advancement both countries reaffirmed in their February 2026 joint statement.
- **Student mobility:** More restrictive migration policies could complicate France's target of welcoming 30,000 Indian students by 2030 and opportunities under the bilateral Migration and Mobility Partnership Agreement.
- **Multilateral engagement:** Domestic instability could reduce France's diplomatic bandwidth for shared priorities, including its reiterated support for India's permanent membership of the United Nations Security Council.

3. On right to internet, Court ruling isn't enough (GS Paper II Governance)

This editorial '**On right to internet, Court ruling isn't enough**' was published in **The Indian Express** on 21st Oct 2026, highlights the need for **institutional safeguards** and **judicial enforcement** to translate online child protection and internet rights into practice.

Online Child Protection

- The **Supreme Court's October 15 ruling** tightened controls on online child sexual exploitation and abuse material, addressing compliance gaps under the **Information Technology Rules**.
- A **national database** of digital identifiers must enable removal of "known-origin" matches without verification; intermediaries must assess even non-explicit content's **exploitation potential**, with hefty fines suggested for non-compliance.
- Stronger **child protection** requires proactive state intervention and an **institutional architecture** governing database use and misuse beyond judicial assurances.

Internet Rights and Enforcement

- Recognising internet access and use under **Articles 19 and 21** enables direct Supreme Court enforcement and subjects future screen-time restrictions to **constitutionally permissible limits**, amid frequent state reliance on shutdowns for policing.
- Expansion of **Article 21** has outpaced effective enforcement; rights to speedy trials, clean air and safer roads illustrate the gap between **judicial recognition** and meaningful remedies.
- Courts must enforce **internet rights** against unreasonable and disproportionate shutdowns through timely **judicial intervention** restraining the state.

Beyond Editorial

Structural Barriers to Universal Internet Access

- **Infrastructure gaps:** Connectivity remains geographically uneven; India's Comprehensive Modular Survey: Telecom, 2025 recorded household internet access at 83.3% in rural areas against 91.6% in urban areas.
- **Affordability constraints:** Low prices do not ensure affordability; International Telecommunication Union data for 2024 found mobile broadband consumed 19 times more income proportionally in low-income than high-income economies.
- **Digital literacy:** Connectivity requires practical skills; the Pradhan Mantri Gramin Digital Saksharta Abhiyan targeted 6 crore rural households for training in internet use, digital payments and government services.
- **Gender disparities:** Unequal device ownership limits independent access; the 2025 telecom survey found mobile ownership among rural adults at 80.7% for men and 48.4% for women.
- **Disability barriers:** Inaccessible verification can block essential services; the Supreme Court's 2025 digital-access judgment addressed eye-blinking requirements that excluded acid attack survivors from completing digital identification procedures.
- **Language exclusion:** Unfamiliar languages restrict meaningful participation; BHASHINI's translation services across 22 scheduled Indian languages illustrate efforts to make digital services more accessible.
- **Institutional exclusion:** Weak school connectivity limits access for children without home facilities; Unified District Information System for Education Plus data recorded internet availability in only 53.9% of schools in 2023–24.