

EDITORIALS – 4TH AUG 2026

1. Proof of life (GS Paper II Governance)

This editorial 'Proof of life' was published in The Hindu on 4th Aug 2026, highlights how stricter control over delayed birth registration may exclude legitimate applicants without proven gains against fraud.

New birth-registration framework

- The Registration of Births and Deaths (Amendment) Bill, 2026 amends Section 13(3) of the 1969 Act after its passage in the Lok Sabha.
- Delays up to two years require an executive magistrate's order, while longer delays require verification and approval by a judicial magistrate.
- The 2023 amendment made birth certificates near-conclusive proof for education, voter enrolment, passports, Aadhaar, driving licences and government jobs.
- It also permitted digital databases shared with the Registrar General, increasing birth certificates' gatekeeping power and incentives for fraud.

Weak justification and exclusion risks

- Lok Sabha passage lacked legislative debate because the Opposition was protesting the police crackdown on the July 20 CJP protests.
- Judicial scrutiny may protect administrators from accusations of arbitrary documentation, but makes erroneous decisions harder for disadvantaged applicants to rectify.
- The Bill retains existing evidentiary standards; stricter documentation could have addressed suspected fraud without mandatory judicial intervention.
- No published evidence shows fraud rising after two years or proves that the judicial threshold is superior to less burdensome alternatives.
- Delays often arise from remote residence or undocumented migration, while applicants may later need birth certificates for educational access.

Underlying policy concern

- The policy prioritises document assurance over accessibility, treating wrongful exclusion as an acceptable cost of preventing wrongful inclusion.

Beyond Editorial

Constitutional safeguards against documentary exclusion

- Proportionality safeguard: The Supreme Court's 2018 Aadhaar judgment applied proportionality to identity regulation, requiring restrictions to pursue legitimate aims through necessary and balanced means.
- Educational protection: Section 14 of the RTE Act expressly prohibits denying school admission for lack of age proof, protecting undocumented children from educational exclusion.
- Alternative evidence: The Central RTE Rules accept hospital, ANM or Anganwadi records and parental declarations when birth certificates are unavailable, offering an inclusive verification model.
- Document hierarchy: In 2024, the Supreme Court clarified that Aadhaar establishes identity but is not proof of date of birth, discouraging excessive dependence on one document.
- Assisted registration: India has nearly three lakh Registrars and Sub-Registrars under the Civil Registration System, which can provide local assistance before applicants approach courts.
- Privacy protection: The DPDP Act, 2023 provides security, correction and grievance safeguards, particularly relevant when birth databases contain sensitive personal data of children.
- Controlled integration: UIDAI's 2025 death-reporting service uses Civil Registration System records for Aadhaar updates, illustrating purpose-specific database linkage instead of unrestricted data sharing.

2. AI and cyber, the double helix of today's security threats (GS Paper III Science and Technology, Security)

This editorial 'AI and cyber, the double helix of today's security threats' was published in The Hindu on 4th Aug 2026, highlights how the convergence of artificial intelligence and cyber threats is transforming warfare, redistributing power and outpacing global safeguards.

Converging security threats

- Growing digital interconnectedness makes AI and cyber risks mutually reinforcing, threatening every level of global security and economic stability.
- AI-powered malware can adapt to environmental changes, evade traditional antivirus systems and make cyberattacks harder to detect and mitigate.

- Malicious autonomous agents can undermine Zero Trust protocols and aggravate insider threats, exposing weaknesses in existing security architecture.
- The Ukraine war shows how emerging technologies create asymmetric advantages capable of disrupting conventional military calculations.
- Governments are combining innovation, policy coherence and strategic realism, but their cyber preparedness continues to lag behind sophisticated digital adversaries.

Agentic AI and changing power structures

- Businesses are rapidly adopting Large Language Models without adequate training or human-interface adaptation, making Agentic AI implementation increasingly complex.
- Anthropic's Mythos reportedly detects zero-day vulnerabilities across major operating systems, exposing the limits of legacy systems.
- In the Russia-Ukraine and U.S.-Israel-Iran conflicts, AI-enabled systems have tracked missile trajectories and extracted intelligence from images, text, radio and electromagnetic signals.
- Autonomous munitions such as Goalkeeper and Whiplash can identify and strike targets independently, raising concerns over human control and civilian safety.
- The World Economic Forum warns that AI may strengthen cyber defence while enabling sophisticated automated attacks that could weaken Zero Trust systems.
- Advanced autonomous agents may give rogue groups capabilities once restricted to states, redistributing military and economic power towards AI leaders.
- Anthropic, Palantir and comparable ecosystems increasingly control advanced technology, while rules governing AI concentration and its use remain underdeveloped.

Governance, reliability and geopolitical risks

- Existing cyber rules may require rewriting as Agentic Autonomous Operations become more capable, autonomous and difficult to contain through present governance frameworks.
- AI hallucinations, subjective judgments and embedded algorithmic bias can produce distorted decisions and encourage algorithmic radicalisation.
- U.S. allegations that China's Moonshot copied Anthropic's Fable model, rejected by China, reflect intensifying U.S.-China competition over frontier AI capabilities.
- If advanced models can outperform most humans in finding and exploiting vulnerabilities, threats could extend across operating systems, cryptographic software and critical infrastructure.

- Defence AI may generate unreliable or nationally biased warnings; retaining human oversight and linking alerts with accurate situational understanding are therefore essential.

Beyond Editorial

India's preparedness for AI-enabled cyber warfare

- Rising threat load: CERT-In handled over 29.44 lakh cyber incidents in 2025 and issued 1,530 alerts, demonstrating the scale confronting India's cyber-defence system.
- Institutional foundation: The Defence AI Council and Defence AI Project Agency were created to accelerate military AI adoption, but require closer tri-service and civilian coordination.
- Indigenous capacity: The ₹10,371.92-crore IndiaAI Mission has onboarded over 38,000 GPUs, providing a base for domestic models and secure defence-grade computing.
- Realistic exercises: Bharat NCX 2025 simulated autonomous malware, deepfake manipulation and critical-infrastructure attacks, improving operational preparedness for AI-enabled cyber crises.
- Model assurance: The IndiaAI Safety Institute and 13 Responsible AI projects cover bias, privacy, explainability and risk assessment, which can inform military AI testing.
- Specialised workforce: The CSPAI programme trains cybersecurity professionals to secure AI systems, providing a model for similar capacity-building across defence and critical infrastructure.
- International cooperation: The 2026 Australia-India partnership covers cybercrime, malicious cyber activity, security norms and critical infrastructure, supporting collective resilience against cross-border threats.

3. Listening to rivers, learning from fires (GS Paper III Disaster Management)

This editorial 'Listening to rivers, learning from fires' was published in The Indian Express on 4th Aug 2026, highlights how climate hazards become disasters through local ecological damage, social vulnerability and weak governance, requiring preventive and place-specific adaptation.

Climate risk and local vulnerability

- Floods in Assam and Asia, Kerala landslides and European fires show that climate change operates through distinct ecologies, histories and social vulnerabilities.
- A warmer atmosphere intensifies rainfall, heat and drought, but disaster impacts depend equally on land use, governance and ecological stewardship.
- Climate change requires societies to reassess risk management, development choices and their relationship with the natural environment.

Lessons from different landscapes

- The Brahmaputra system naturally reshapes channels and floods plains, while embankments restrict river movement and worsen damage when flood limits are exceeded.
- More intense rainfall and catchment degradation weaken water regulation and soil retention, increasing Assam's flood vulnerability.
- Assam's recurring floods expose the limits of relief-based governance, requiring vulnerability reduction before disasters rather than repeated post-disaster rehabilitation.
- Kerala's landslide losses are intensified by quarrying, deforestation, roads and hillside habitation, reflecting weak adherence to the Western Ghats Ecology Expert Panel and poor ecological planning.
- Mediterranean fire risk has risen through warming, drought and heatwaves, while rural decline, reduced grazing and prolonged fire suppression have increased combustible vegetation accumulation.
- Expansion of housing and tourism into fire-prone landscapes further converts natural hazards into severe human disasters.

Governance and adaptation

- Climate-attribution studies and satellite monitoring can identify warming influences, but cannot alone explain why similar hazards produce unequal consequences.
- India must strengthen disaster anticipation while rethinking the governance of rivers, forests, mountains and cities under a changing climate.
- Urban planning and public infrastructure must reflect evolving landscape risks, rather than relying on past climatic and hydrological patterns.
- Since disasters vary across regions, climate adaptation must use locally grounded responses instead of a uniform blueprint.

Beyond Editorial

Financing locally led climate adaptation

- **Response dominance:** For 2021–26, States received ₹1,28,122.4 crore for disaster response but ₹32,030.6 crore for mitigation, revealing the greater fiscal weight given to post-disaster expenditure.
- **Local mitigation:** The Fifteenth Finance Commission explicitly permitted mitigation funds for community-level interventions and environment-friendly settlements, providing a basis for direct local adaptation grants.
- **Ecosystem investment:** A Green Climate Fund project covers 24 coastal ecosystems across Andhra Pradesh, Maharashtra and Odisha, demonstrating finance-led protection of vulnerable coastal communities.
- **Wetland resilience:** A National Adaptation Fund project proposed restoring Mahanadi catchment wetlands in Chhattisgarh to strengthen climate-resilient livelihoods and local natural-resource management.
- **Risk insurance:** Nagaland's 2024–27 parametric insurance programme uses rainfall triggers to finance rapid disaster response and protect critical infrastructure without awaiting conventional damage assessment.
- **Budget tagging:** Odisha's Climate Budget 2025–26 uses Climate Change Impact Appraisal to identify climate-relevant expenditure and assess whether development schemes remain resilient.
- **Targeted funding:** The Fifteenth Finance Commission earmarked ₹11,950 crore for priorities such as urban flooding, landslides, drought and erosion, linking finance with identified local risks.