PrepAlpine

The Next-Generation UPSC Institution

Where Research Meets Mentorship & Precision

Preparation Meets Precision

A Next-Generation Learning Institution

Disclaimer

The information contained in this book has been prepared solely for educational purposes. While every effort has been made to ensure accuracy, PrepAlpine makes no representations or warranties of any kind and accepts no liability for any errors or omissions. The use of any content is solely at the reader's discretion and risk.

First Edition: January 2026

Printed and published by PrepAlpine

DAILY CURRENT AFFAIRS DATED 14.01.2026

GS Paper I: Society

1. Urbanisation of Small Towns in India: Nature, Drivers and Challenges

a. India's Changing Urban Landscape

i. Rethinking India's Urbanisation Narrative

Urbanisation in India is often visualised through metropolitan cities such as Delhi, Mumbai, or Bengaluru. While these cities dominate popular imagination and policy focus, they represent only a small fraction of India's urban reality.

Out of nearly nine thousand statutory and census towns, fewer than five hundred qualify as large cities. The overwhelming majority are small towns with populations below one lakh. It is within these settlements that demographic transition, labour mobility, and economic diversification are unfolding most rapidly.

India, therefore, is not merely urbanising through megacities; it is urbanising primarily through small towns. This shift fundamentally reshapes questions of governance, infrastructure, labour markets, and social equity.

ii. Are India's Small Towns Truly Urbanising?

Small towns are undoubtedly part of India's urban transition, but their urbanisation follows a distinct and uneven trajectory. They are no longer rural in character, yet they do not evolve like planned cities.

- **Functional Transformation:**
  Small towns increasingly function as market centres, transport and logistics nodes, agro-processing hubs, warehousing points, and service clusters linked to construction and retail.
- **Labour Absorption:**
  They absorb rural youth exiting agriculture as well as migrants pushed out of metropolitan cities due to rising costs of living and housing.
- **Institutional Deficit:**
  This growth occurs largely without adequate planning frameworks, infrastructure investment, or administrative capacity.

As a result, small-town urbanisation remains structurally weak, spatially uneven, and socially vulnerable, shaped more by market forces than by institutional design.

b. Drivers Behind the Shift from Metropolitan Cities

i. Crisis of Metropolitan Over-Accumulation

The movement of capital and labour away from large cities is not accidental. It reflects the growing crisis of metropolitan over-concentration.

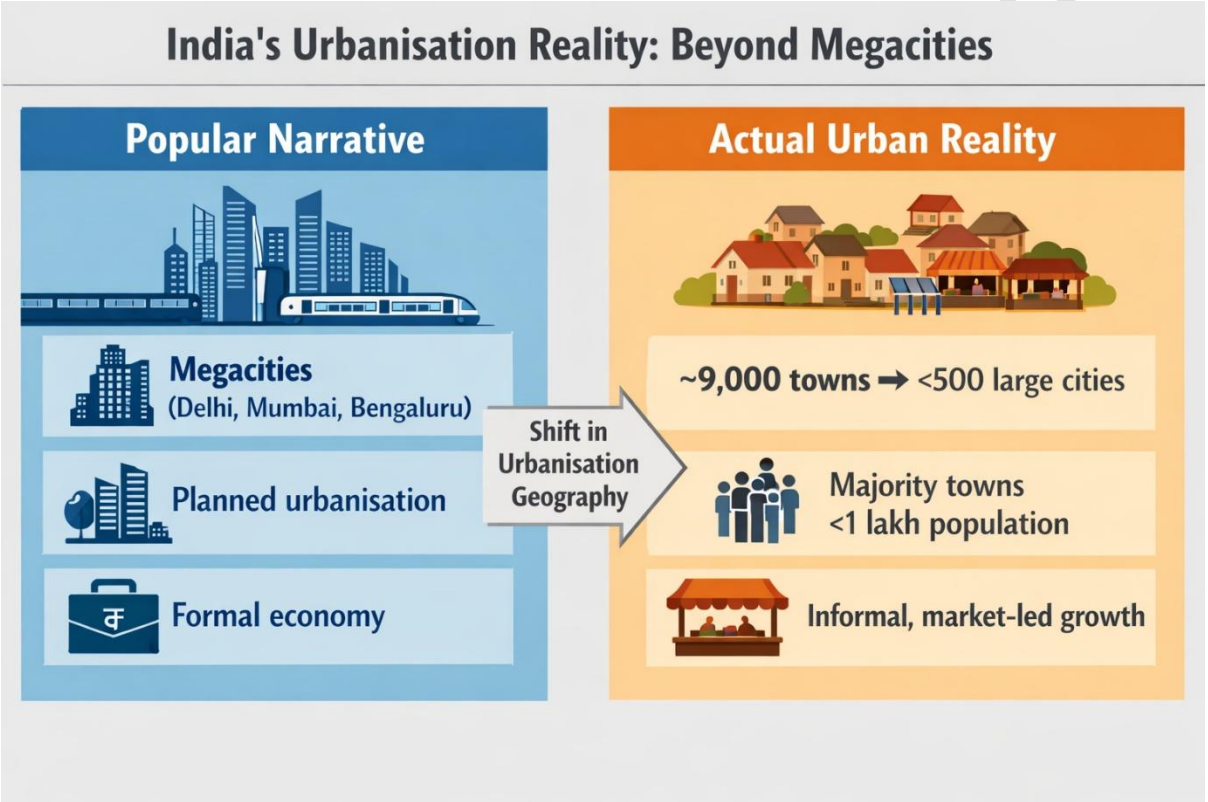
- **Rising Urban Stress:**
  Metro cities face sharply escalating land prices, overloaded infrastructure, unaffordable housing, congestion, and environmental degradation.
- **Exclusion of Informal Workers:**
  Low-income and informal workers are increasingly priced out of metropolitan spaces, making everyday urban survival difficult.
- **Capital Relocation:**
  Firms and investors seek smaller towns where land is cheaper, labour is more flexible, and regulatory oversight is weaker.

Small towns thus emerge not as outcomes of planned decentralisation, but as spaces of economic adjustment, absorbing pressures generated by metropolitan saturation.

ii. Are Small Towns a Natural Alternative to Big Cities?

Small towns do not inherently resolve the problems associated with metropolitan urbanisation. In many cases, they reproduce similar inequalities in a more compressed and precarious form.

- **Dominance of Informal Labour:**
  Construction workers lack contracts and social security, women are concentrated in home-based piece-rate work, and youth are absorbed into unstable gig and platform-based employment.
- **Emergence of New Power Structures:**
  Control over land, finance, and labour is consolidated by real estate intermediaries, contractors, micro-finance agents, and local political brokers.
- **Urbanisation of Poverty:**
  Rather than inclusive growth, many small towns experience the migration of rural insecurity into urban spaces without corresponding improvements in dignity, rights, or services.



c. Structural Constraints in Small-Town Urbanisation

i. Infrastructure Deficits and Policy Bias

A persistent policy bias in favour of large cities severely constrains small towns.

- **Metro-Centric Urban Schemes:**
  Major programmes such as AMRUT prioritise large-scale, centralised infrastructure models that exceed the fiscal and administrative capacity of small municipalities.
- **Fragmented Service Provision:**
  Small towns depend on ad hoc schemes, temporary arrangements, and under-maintained infrastructure.
- **Environmental Stress:**
  Water supply often relies on tankers, groundwater extraction intensifies, and local ecosystems face growing pressure.

Infrastructure deficits thus emerge as both developmental bottlenecks and environmental risks.

ii. Weaknesses in Urban Governance

Urban governance structures in small towns remain deeply constrained.

- **Limited Fiscal Capacity:**
  Municipal bodies suffer from inadequate revenue sources and insufficient fiscal devolution.
- **Administrative Shortages:**
  There is a lack of trained technical and planning personnel within local bodies.
- **Tokenistic Participation:**
  Although public participation is formally mandated, it often remains procedural rather than substantive, weakening accountability and local ownership.

From a governance perspective, small-town urbanisation exposes systemic gaps in fiscal federalism, administrative capacity, and democratic decentralisation.

d. Overall Character of Small-Town Urbanisation

In essence, small-town urbanisation in India is predominantly unplanned and market-led.

- Labour remains informal and insecure.
- Governance institutions are weak and under-resourced.
- Infrastructure provision is fragmented.
- Social outcomes increasingly reflect new forms of inequality.

Rather than acting as engines of balanced development, many small towns risk becoming sites of entrenched vulnerability.

e. Way Forward: Towards Sustainable Small-Town Urbanisation

A sustainable response begins with recognising small towns as central to India's urban future, not as transitional or residual spaces.

- **Context-Specific Planning:**
  Urban planning must integrate housing, livelihoods, transport, and local ecological conditions instead of replicating metropolitan models.
- **Strengthening Municipal Institutions:**
  Enhanced fiscal devolution, professional staffing, and transparent budgeting are essential for effective local governance.
- **Protecting Urban Labour:**
  Institutional spaces for worker collectives, cooperatives, and informal-sector representation can improve security and bargaining power.
- **Regulating Capital and Platforms:**
  Real estate speculation and platform-based economies must be regulated to retain locally generated economic value and safeguard labour rights.

Conclusion

Small towns are not peripheral to India's urbanisation; they lie at its very core. Yet their current trajectory reflects stress-driven expansion rather than planned transformation. Without empowered municipalities, inclusive planning frameworks, and effective labour protection mechanisms, small towns risk becoming new centres of inequality rather than drivers of balanced growth. Addressing this challenge is essential for achieving sustainable, equitable, and resilient urbanisation in India.

GS Paper II: Current Affairs

2. Government Access to Smartphone Source Code: Concept, Concerns and the Way Forward

a. Growing Importance of the Issue in the Digital Age

In the contemporary digital ecosystem, smartphones are no longer mere communication devices. They function simultaneously as financial instruments, identity gateways, data repositories, and access points for government and private services.

- Digital payments, biometric authentication, and e-governance services increasingly rely on smartphones.
- Devices store sensitive personal data such as messages, financial records, health information, and precise location histories.
- Encrypted communication and cloud integration make smartphones integral to both personal and institutional security.

Given this centrality, concerns regarding hidden vulnerabilities, malicious backdoors, or unsafe pre-installed software have intensified. Governments across the world are therefore debating whether access to smartphone source code is necessary to ensure public safety, cybersecurity, and national security.

b. Understanding Source Code and Its Significance

Source code refers to the original set of instructions written by software developers that determines how a digital device functions.

- It controls how data is stored, processed, and transmitted.
- It defines security mechanisms such as encryption, permissions, and access controls.
- It governs how the operating system interacts with applications and external servers.

Without source code, software cannot operate. Conversely, access to source code allows complete visibility into a device's internal logic, data flows, and security architecture. This makes source code both extremely valuable and extremely sensitive.

c. Why Companies Strongly Protect Source Code

Technology firms protect source code for both economic and cybersecurity reasons.

- **Intellectual Property Protection:**
  Source code represents years of research, innovation, and financial investment. Mandatory disclosure risks imitation, reverse engineering, and loss of competitive advantage.
- **Security Through Controlled Access:**
  Limiting visibility itself functions as a defensive layer. If internal software logic is widely exposed, attackers gain a detailed roadmap to identify vulnerabilities.
- **Risk of Misuse:**
  Once source code leaves a controlled environment, the ability to prevent copying, leakage, or misuse becomes significantly weaker.

Thus, greater visibility does not automatically translate into greater security. In certain contexts, indiscriminate disclosure may actually weaken cybersecurity.

d. Global Practice on Government Access to Source Code

As a general rule, governments do not demand permanent or unrestricted access to the source code of commercial consumer devices.

- Security assurance is typically achieved through certification, compliance testing, and audit outcomes.
- Full code access is limited to exceptional sectors such as defence systems or critical national infrastructure.
- Even in such cases, access is granted under strict legal safeguards, secure facilities, and confidentiality obligations.

Globally, the emphasis has been on verifying security outcomes, not on acquiring or retaining proprietary software code.

e. Why Government Demand for Source Code Is Controversial

Proposals for government access to smartphone source code raise multiple challenges.

- **Cybersecurity Risks:**
  Centralised handling or storage of sensitive code creates high-value targets for hackers. If regulatory bodies or testing agencies lack robust security infrastructure, the risk of leaks or breaches increases.
- **Privacy Concerns:**
  Expanded access to underlying software architecture fuels apprehensions about surveillance, misuse of personal data, and erosion of the right to privacy, which is closely tied to constitutional principles and accountable governance.
- **Impact on Innovation and Investment:**
  Regulatory uncertainty and intrusive requirements may discourage firms from introducing new technologies or investing in advanced research, weakening the digital ecosystem.

f. Does Greater Code Visibility Automatically Improve Security?

Cybersecurity experts broadly agree that complete exposure of source code does not inherently strengthen security.

- Effective cybersecurity relies on layered protection, restricted access, and continuous monitoring.
- Controlled audits, sandbox testing, and vulnerability assessments in secure environments are often more effective.
- Excessive exposure of core software logic can increase the attack surface, especially in complex consumer technologies like smartphones.

Security, therefore, depends more on processes and safeguards than on unrestricted transparency.

g. The Government's Perspective and Legitimate Concerns

From the state's viewpoint, the issue is grounded in public interest.

- Unsafe software can expose citizens to fraud, identity theft, and data breaches.
- Hidden backdoors or malicious applications may facilitate foreign surveillance or cyber-espionage.
- Smartphones increasingly support critical functions in finance, governance, and public services.

The core debate, therefore, is not about whether the state has a role, but about how far and in what manner that role should extend.

h. Stakeholders and Competing Interests

- Governments prioritise national security and consumer protection.
- Technology companies emphasise intellectual property rights and business sustainability.
- Citizens seek privacy, trust, and digital safety.
- Digital rights groups advocate transparency, accountability, and proportional regulation.

The policy challenge lies in balancing these interests without disproportionately privileging one at the expense of others.

i. Way Forward: Towards a Balanced Regulatory Approach

A viable solution lies in outcome-based regulation rather than ownership or custody of source code.

- **Security Benchmarks:**
  Governments can mandate compliance with clearly defined cybersecurity standards without demanding unrestricted access.
- **Controlled Audits:**
  Independent, high-security testing laboratories can conduct audits without permanent retention or duplication of code.
- **Transparent Rule-Making:**
  Public consultation, clear legal safeguards, and judicial oversight are essential to maintain legitimacy and trust.
- **Global Alignment:**
  Harmonisation with international best practices prevents regulatory isolation and supports innovation while strengthening cybersecurity resilience.

Conclusion

Government access to smartphone source code lies at a delicate intersection of security, privacy, and technological innovation. While the state has a legitimate responsibility to protect citizens and national interests, unchecked or disproportionate access risks creating vulnerabilities greater than those it seeks to prevent. A transparent, proportionate, and globally aligned regulatory framework is therefore essential to preserve public trust, enhance cybersecurity, and sustain long-term digital progress.

GS Paper III: Environment

3. Artificial Intelligence and Its Environmental Impact

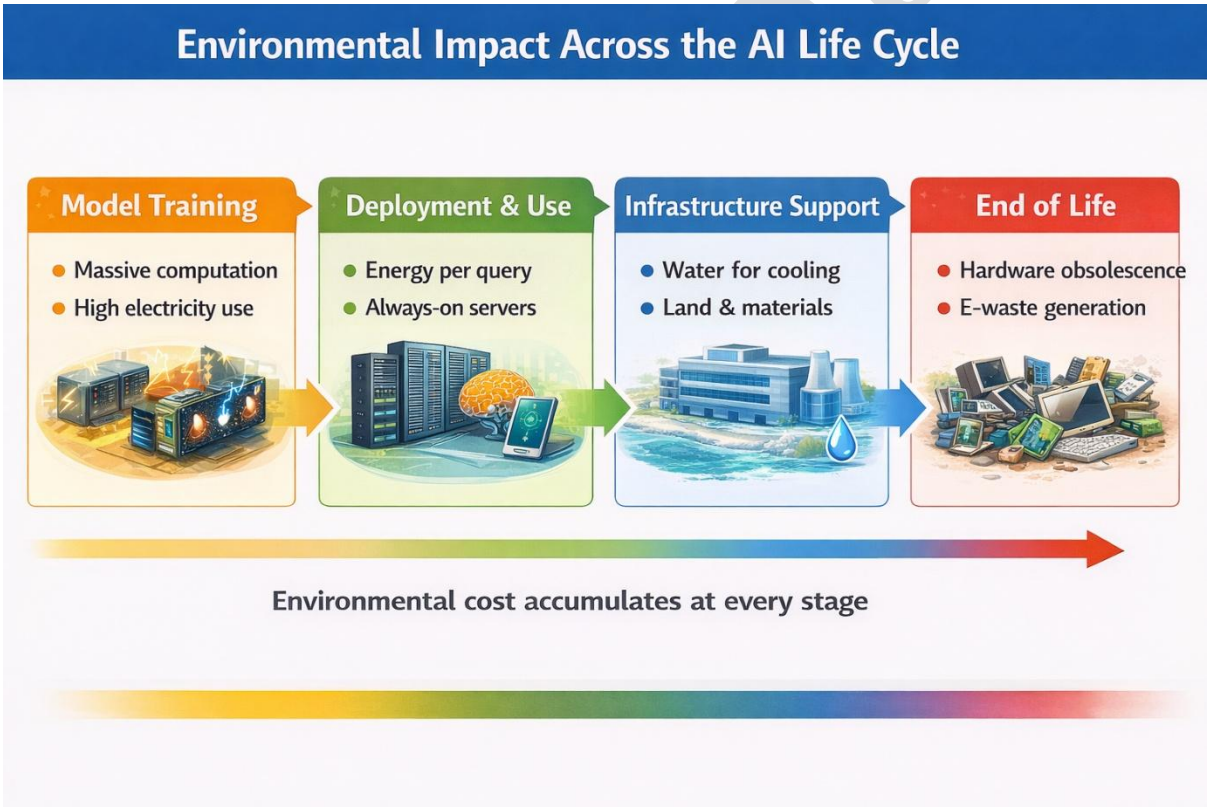
a. Artificial Intelligence and the Sustainability Question

Artificial Intelligence has moved rapidly from a specialised technological field to a foundational infrastructure shaping modern societies. It is now embedded in healthcare diagnostics, agricultural forecasting, education platforms, financial systems, governance processes, and national security architectures. India, too, views Artificial Intelligence as a key driver of productivity, efficiency, and economic growth.

However, the dominant narrative surrounding Artificial Intelligence focuses almost entirely on its benefits and strategic potential. The environmental costs associated with its development and deployment remain largely invisible in public discourse.

In reality, Artificial Intelligence systems rely on energy-intensive computation, water-intensive cooling mechanisms, and resource-heavy digital infrastructure. These dependencies contribute to carbon emissions, ecological stress, and climate change.

Understanding the environmental footprint of Artificial Intelligence is therefore essential if technological progress is to remain aligned with sustainability, responsible governance, and intergenerational equity.



b. Environmental Impact Across the AI Life Cycle

i. Energy Consumption

Artificial Intelligence systems require vast computational power, provided by high-performance servers housed in large data centres.

- Training large AI models involves repeated processing of massive datasets, consuming significantly more electricity than conventional digital services.

- Even routine use of AI-enabled applications often requires higher energy per query compared to traditional internet searches.
- As model complexity increases, energy demand rises proportionately.

At its core, Artificial Intelligence is computationally intensive, and higher computational complexity directly translates into higher energy consumption.

ii. Carbon Emissions

Much of the electricity powering global data centres continues to be generated from fossil fuels.

- Training a single large AI model can generate carbon emissions running into hundreds of thousands of kilograms of carbon dioxide.
- Continuous scaling of AI across sectors magnifies cumulative emissions.
- These emissions undermine climate mitigation efforts and sustainable development goals.

As Artificial Intelligence expands, its carbon footprint increasingly resembles that of energy-intensive industrial sectors.

iii. Water Consumption

Artificial Intelligence infrastructure depends heavily on freshwater resources.

- Data centres require large volumes of water for cooling servers and preventing overheating.
- Globally, AI-driven data centres consume billions of cubic metres of water annually.
- This intensifies stress in water-scarce regions, aggravating resource competition.

The environmental burden of Artificial Intelligence thus extends into questions of water security and environmental justice.

iv. Land Use and Electronic Waste

- Expansion of data centres requires land, construction materials, and supporting infrastructure, often altering local land-use patterns.
- AI hardware such as servers and processors has a limited operational lifespan.
- Rapid technological obsolescence generates large quantities of electronic waste containing toxic components.

Improper disposal of e-waste contaminates soil, water bodies, and ecosystems, creating long-term environmental hazards.

c. Global Recognition of AI's Environmental Costs

International institutions increasingly recognise that Artificial Intelligence is not environmentally neutral.

- UNESCO's 2021 Ethics of Artificial Intelligence framework explicitly identifies environmental harm as a key ethical concern.
- The United Nations Environment Programme has highlighted AI's life-cycle environmental footprint.
- The OECD has emphasised the need for systematic measurement of AI-related environmental impacts.

Regulatory responses are also emerging.

- The European Union has introduced transparency requirements related to emissions from data centres.
- Legislative discussions in the United States increasingly address environmental dimensions of advanced digital technologies.

These developments signal that AI governance must extend beyond data and ethics to include sustainability.

d. India's Current Policy Approach

In India, Artificial Intelligence policy discussions are largely framed around innovation, competitiveness, and digital public infrastructure.

- Environmental costs associated with AI are neither systematically measured nor explicitly regulated.
- Large-scale data centres and AI infrastructure remain largely outside environmental regulatory scrutiny.

A major gap exists within India's Environmental Impact Assessment framework. The EIA Notification of 2006 focuses on industrial, mining, and physical infrastructure projects, while AI infrastructure remains largely excluded. As a result, environmental consequences of AI expansion escape formal assessment.

e. Importance of Measuring AI's Environmental Impact

Without reliable measurement, the environmental costs of Artificial Intelligence remain invisible.

- Policymakers lack credible data to design effective regulations.
- Fragmented estimates weaken accountability and public awareness.
- Environmental harm remains externalised.

Effective governance requires clear metrics covering energy use, carbon emissions, water consumption, material intensity, and life-cycle impacts across both training and deployment phases.

Measurement is the foundation upon which credible regulation and responsible innovation must rest.

f. Role of Standards and Disclosure Mechanisms

- Uniform standards are essential for comparability and credibility of environmental impact assessments.
- Common indicators and reporting frameworks should be developed through collaboration among industry, academia, and environmental institutions.
- AI-related environmental impacts can be integrated into Environmental, Social and Governance disclosure norms.

In India, institutions such as the Ministry of Corporate Affairs and the Securities and Exchange Board of India can mandate transparency, aligning digital innovation with responsible business conduct.

g. Towards Sustainable Artificial Intelligence

Reducing AI's environmental footprint does not require abandoning technological progress.

- Algorithmic efficiency can be improved by optimising models and reusing pre-trained systems.
- Data centres can transition towards renewable energy and water-efficient cooling technologies.
- Artificial Intelligence itself can support environmental protection through climate modelling, energy optimisation, and resource management.

Sustainability and innovation are therefore complementary rather than conflicting goals.

h. Way Forward for India

- AI infrastructure should be recognised as an environmental governance issue, not merely a technological domain.
- Large data centres should be brought within environmental assessment frameworks.

- India must develop standardised systems for measuring AI-related environmental impacts aligned with global best practices.
- Mandatory disclosure of AI-related emissions and resource use should be incorporated into corporate reporting norms.
- India's AI strategy must align with the Sustainable Development Goals, particularly those related to climate action and responsible consumption.

Conclusion

Artificial Intelligence holds immense promise for economic development and social transformation. However, unchecked expansion carries significant environmental risks that cannot be ignored. India must move beyond viewing Artificial Intelligence solely as a growth engine and confront its hidden ecological costs. By measuring impacts, strengthening regulation, and promoting sustainable AI practices, technological advancement can be harmonised with environmental sustainability and intergenerational justice.

Reader's Note — About This Current Affairs Compilation

Dear Aspirant,

This document is part of the PrepAlpine Current Affairs Series — designed to bring clarity, structure, and precision to your daily UPSC learning.

While every effort has been made to balance depth with brevity, please keep the following in mind:

1. Orientation & Purpose

This compilation is curated primarily from the UPSC Mains perspective — with emphasis on conceptual clarity, analytical depth, and interlinkages across GS papers.

However, the PrepAlpine team is simultaneously developing a dedicated Prelims-focused Current Affairs Series, designed for:

- factual coverage
- data recall
- Prelims-style MCQs
- objective pattern analysis

This Prelims Edition will be released separately as a standalone publication.

2. Content Length

Some sections may feel shorter or longer depending on topic relevance and news density.
To fit your personal preference, you may freely resize or summarize sections using any LLM tool (ChatGPT, Gemini, Claude, etc.) at your convenience.

3. Format Flexibility

The formatting combines:

- paragraphs
- lists
- tables
- visual cues

—all optimised for retention.

If you prefer a specific style (lists → paras, paras → tables, etc.), feel free to convert using any free LLM.

4. Monthly Current Affairs Release

The complete Monthly Current Affairs Module will be released soon, optimized to a compact 100–150 pages — comprehensive yet concise, exam-ready, and revision-efficient.