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.

DAILY CURRENT AFFAIRS DATED 04.05.2026

GS Paper III: Security

1. Dual-Use Satellites and Modern Space Warfare

a. Introduction: The Changing Nature of Space Conflict

Earlier, outer space was largely associated with scientific exploration, satellite communication, weather forecasting, and peaceful international cooperation. However, in the 21st century, space has increasingly emerged as a critical strategic domain connected with:

- national security,
- digital governance,
- economic systems,
- military operations,
- financial networks,
- and communication infrastructure.

Today, modern societies depend heavily upon satellites for daily functioning. Consequently, space warfare is no longer limited to dramatic missile attacks against satellites. Instead, conflicts are gradually shifting toward invisible and digitally driven methods of disruption.

Future wars may therefore begin not with explosions, but with:

- collapse of navigation systems,
- disruption of internet connectivity,
- breakdown of banking networks,
- failure of emergency communication,
- interference with drones and missiles,
- or manipulation of digital infrastructure.

Thus, modern space warfare is increasingly linked with:

- cyber warfare,
- information warfare,
- electronic warfare,
- and critical infrastructure security.

This transformation has made outer space one of the most strategically sensitive domains of contemporary geopolitics.

b. Understanding Dual-Use Satellites

Meaning of Dual-Use Satellites

Dual-use satellites are satellites that simultaneously perform both civilian and military functions.

In simple terms, the same satellite system that supports ordinary civilian life may also assist military operations during conflict.

For example:

Civilian Use	Military Use
GPS navigation	Missile guidance

Civilian Use	Military Use
Internet services	Battlefield communication
Weather forecasting	Military planning
Disaster warnings	Surveillance operations
Banking synchronisation	Secure defence coordination

Thus, a satellite helping civilians use navigation maps may also help military drones accurately identify targets.

Similarly, communication satellites providing internet services may simultaneously support defence communication networks.

Why Dual-Use Satellites Create Strategic Complexity

Traditional international law was built upon a clear distinction between:

- civilian objects, which must be protected during war, and
- military targets, which may be attacked.

However, dual-use satellites blur this distinction.

A single satellite may simultaneously:

- support civilian aviation,
- enable online banking,
- provide weather information,
- and transmit military intelligence.

This creates an important legal and ethical dilemma:

If a civilian satellite also assists military operations, can it become a legitimate military target?

This question lies at the centre of modern debates on space warfare and international humanitarian law.

c. Evolution of Space Warfare

i. From Kinetic Warfare to Non-Kinetic Warfare

Earlier ideas of space warfare focused mainly on kinetic attacks.

Meaning of Kinetic Attacks

Kinetic attacks involve physical destruction through force.

Examples include:

- anti-satellite missiles (ASATs),
- explosive attacks,
- or direct collision with satellites.

Such attacks physically destroy satellites and often create dangerous space debris.

However, modern warfare is increasingly shifting toward non-kinetic methods.

Meaning of Non-Kinetic Warfare

Non-kinetic warfare refers to methods that disable or manipulate systems without physically destroying them.

These methods aim to:

- disrupt communication,
- manipulate signals,
- disable navigation systems,
- or interfere with digital infrastructure.

This shift has occurred because non-kinetic attacks:

- create less visible escalation,
- allow plausible deniability,
- avoid large debris generation,
- and remain below the threshold of open war.

Thus, space warfare is becoming increasingly silent, digital, and ambiguous.

ii. Major Methods of Non-Kinetic Space Attacks

Jamming

Jamming means deliberately interfering with satellite communication signals.

As a result:

- GPS services may fail,
- drones may lose connectivity,
- military communication may collapse,
- and navigation systems may become unreliable.

For example, aircraft or ships relying upon satellite navigation may suddenly lose accurate positioning information.

Spoofing

Spoofing means sending false signals in order to deceive navigation systems.

Unlike jamming, which blocks signals, spoofing manipulates them.

Consequently:

- ships may appear at false locations,
- aircraft may receive incorrect directions,
- or drones may be redirected.

Spoofing is especially dangerous because users may not immediately realise that the information being received is false.

Cyber Hacking

Cyberattacks may target:

- satellite software,
- communication systems,
- ground stations,
- or command-and-control networks.

A successful cyberattack can:

- disable satellites,
- steal intelligence data,
- manipulate imagery,
- or disrupt defence coordination.

Since satellites are closely connected with terrestrial digital infrastructure, cyber vulnerabilities on Earth can directly affect systems in space.

d. Importance of Satellites in Everyday Life

Modern societies are deeply dependent on satellite infrastructure.

Satellites support:

- mobile communication,
- internet connectivity,
- digital payments,
- stock exchanges,
- aviation systems,
- maritime navigation,
- disaster management,
- weather forecasting,
- agricultural monitoring,
- and military operations.

For example:

- banking networks require accurate satellite timing,
- aircraft depend upon satellite navigation,
- and disaster-warning systems rely on satellite communication.

Therefore, satellites are no longer isolated scientific assets. They have become part of critical national infrastructure.

This means disruption of space systems can produce cascading failures across multiple sectors simultaneously.

e. Space Warfare and International Law

i. The Outer Space Treaty, 1967

The Outer Space Treaty is the foundational legal framework governing outer space activities.

It promotes:

- peaceful use of outer space,
- international cooperation,

- and non-weaponisation of celestial bodies.

However, the treaty was drafted during the Cold War era, long before the emergence of:

- cyber warfare,
- private satellite constellations,
- artificial intelligence,
- and large-scale digital dependency.

As a result, many contemporary challenges remain insufficiently addressed under existing international law.

ii. International Humanitarian Law and Dual-Use Problems

International Humanitarian Law (IHL) requires distinction between:

- civilian targets, and
- military targets.

However, dual-use satellites blur this distinction.

For example:

- A civilian communication satellite may also transmit military intelligence.
- A navigation satellite used for transportation may also guide missiles.

This creates uncertainty regarding:

- legitimacy of attacks,
- proportionality,
- civilian harm,
- and military necessity.

Thus, modern space warfare challenges traditional legal categories.

iii. Does Cyberattack in Space Amount to "Use of Force"?

UN Charter Article 2(4)

Article 2(4) of the UN Charter prohibits the use of force against another state.

However, uncertainty exists regarding cyber operations in space.

Important questions arise:

- Does hacking a satellite amount to use of force?
- Is jamming equivalent to armed attack?
- Can cyber disruption justify self-defence under Article 51?

At present, international law does not provide universally accepted answers.

This legal ambiguity increases strategic instability in space relations.

f. The Attribution Problem

i. Meaning of Attribution

Attribution means identifying the actual source of an attack.

In cyber-space warfare, attackers may hide their identity through:

- proxy servers,
- malware routed through multiple countries,
- fake digital identities,
- or use of non-state actors.

As a result, determining the real attacker becomes extremely difficult.

This challenge is known as the attribution gap.

ii. Consequences of Attribution Gap

The attribution problem creates several security challenges:

- **Weakens Deterrence:** Countries may hesitate to retaliate if they cannot conclusively identify the attacker.
- **Encourages Grey-Zone Warfare:** Hostile actors exploit ambiguity to conduct deniable operations.
- **Increases Strategic Confusion:** False accusations or miscalculation may escalate tensions between states.
- **Makes Punishment Difficult:** Without reliable attribution, legal accountability becomes weak.

Thus, ambiguity itself becomes a strategic weapon in modern warfare.

g. Rise of Grey-Zone Warfare

Meaning of Grey-Zone Warfare

Grey-zone warfare refers to hostile actions conducted below the threshold of conventional war.

These operations are designed to create pressure without triggering full-scale military conflict.

Examples include:

- cyberattacks,
- electronic interference,
- spoofing,
- information warfare,
- signal disruption,
- and deniable operations.

Objectives of Grey-Zone Operations

The aim is often not total destruction but gradual weakening of the adversary through:

- confusion,
- disruption,
- psychological pressure,
- governance instability,
- and erosion of public confidence.

Grey-zone warfare is particularly dangerous because it remains difficult to classify legally and strategically.

h. Why Space Warfare Matters for India

India is rapidly emerging as a major space power.

Its satellite infrastructure supports:

- NavIC navigation services,
- defence communication,
- border surveillance,
- weather forecasting,
- disaster management,
- agriculture,
- financial systems,
- and digital governance.

At the same time, India is witnessing increasing participation of private companies in the space sector.

Consequently, India's space security challenge now extends beyond protecting satellites in orbit. It also includes protection of:

- launch infrastructure,
- ground stations,
- communication networks,
- software systems,
- and commercial space assets.

i. Major Challenges Before India

Cyber Vulnerability

Satellite systems remain vulnerable to:

- hacking,
- malware,
- electronic warfare,
- jamming,
- and spoofing.

Attribution Difficulty

Sophisticated cyberattacks may make identification of attackers extremely difficult.

Dual-Use Complexity

The overlap between civilian and military functions complicates:

- defence planning,
- legal interpretation,
- and operational response.

Legal Ambiguity

Existing international legal frameworks remain inadequate for regulating cyber-space warfare.

Commercial Dependence

Private satellite operators may become strategic targets during crises.

Need for Real-Time Monitoring

India requires advanced systems for:

- space situational awareness,
- cyber monitoring,
- signal intelligence,
- and rapid threat detection.

j. India's Way Forward

Secure-by-Design Space Architecture

Cybersecurity must be integrated into satellite systems from the design stage itself.

Security cannot remain an afterthought.

Strengthening Space Cybersecurity

India must improve protection of:

- ground stations,
- satellite software,
- command systems,
- and communication channels.

Regular cyber audits, encryption systems, and secure protocols are essential.

Building Attribution Capacity

India needs advanced technological capability for:

- cyber forensics,
- signal analysis,
- artificial intelligence-based monitoring,
- and rapid identification of suspicious activity.

Improved attribution strengthens deterrence and response capability.

Developing International Norms

India should actively support international efforts to establish:

- responsible behaviour in space,
- norms against attacks on civilian infrastructure,
- and legal clarity regarding cyber operations in space.

This is important for maintaining long-term strategic stability.

Creating Resilience and Redundancy

Critical services should not depend upon a single satellite network.

India must develop:

- backup communication systems,
- distributed satellite constellations,
- resilient infrastructure,

- and alternative navigation systems.

This reduces vulnerability during attacks.

Strengthening Public-Private Coordination

With growing commercial participation in space activities, private operators must follow national security standards.

India therefore requires:

- regulatory oversight,
- information-sharing systems,
- cyber response coordination,
- and integrated security frameworks.

Conclusion

Modern space warfare is becoming increasingly silent, digital, and ambiguous. The battlefield is no longer confined to physical destruction of satellites. Instead, conflicts are gradually shifting toward cyber disruption, electronic interference, signal manipulation, and attacks on critical digital infrastructure.

Dual-use satellites have blurred the traditional distinction between civilian and military assets, creating complex legal, ethical, and strategic challenges for the international community.

For India, space security is no longer only about protecting satellites in orbit. It is equally about protecting:

- economic stability,
- digital governance,
- critical infrastructure,
- national security,
- and everyday civilian life dependent upon satellite systems.

In the coming decades, the countries that successfully combine technological innovation, cyber resilience, legal preparedness, and strategic vision will play a decisive role in shaping the future governance and balance of power in outer space.

GS Paper IV: Disaster Management

2. India's Cell Broadcast Emergency Alert System

a. Introduction: Why Early Warning Systems Matter

One of the most important principles of modern disaster management is:

"Early warning saves lives."

In disasters, the speed at which information reaches people often determines:

- the number of casualties,
- scale of panic,
- efficiency of evacuation,
- and effectiveness of emergency response.

Whether the threat is:

- a cyclone,
- flash flood,
- earthquake,
- industrial accident,
- chemical leak,
- or terror attack,

timely communication can significantly reduce damage and loss of life.

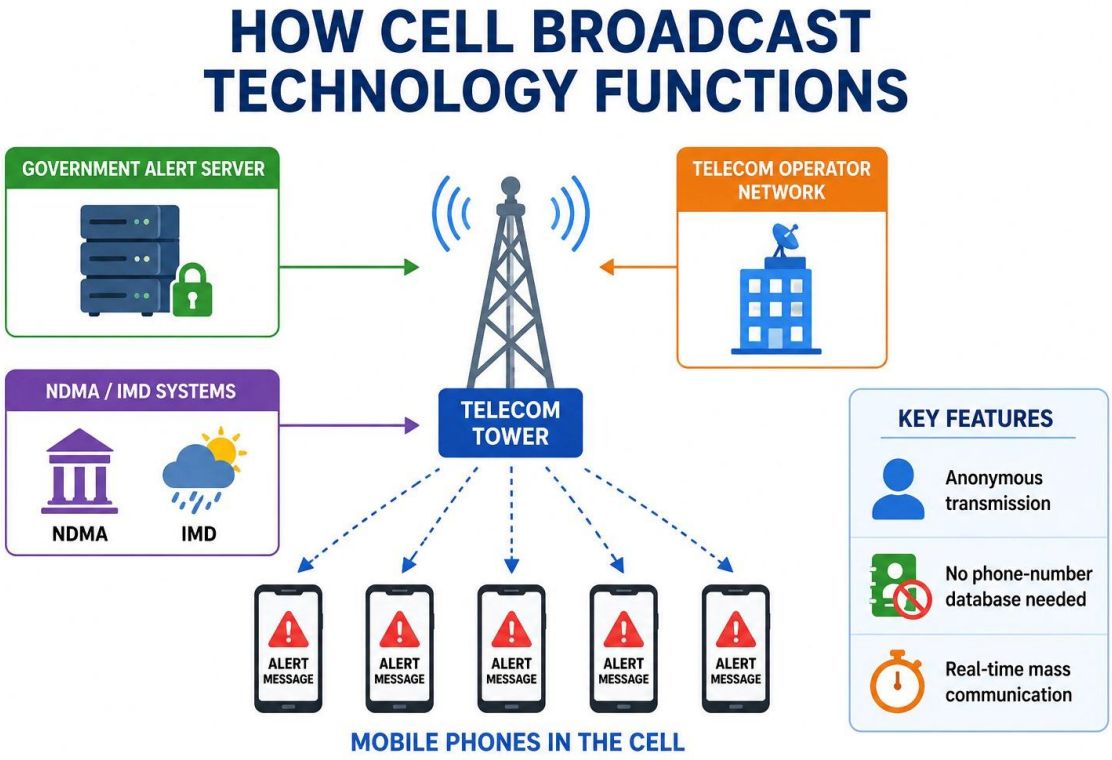
India is now developing a nationwide emergency communication framework based on Cell Broadcast Technology (CBT) to provide rapid alerts during disasters and emergencies.

Recently, millions of mobile users across India received loud warning sounds, vibrations, and "Extremely Severe Alert" notifications as part of a nationwide testing exercise. These demonstrations reflected India's effort to create a modern public-warning infrastructure capable of reaching citizens within seconds.

The importance of such systems is increasing because:

- climate-related disasters are becoming more frequent,
- urban populations are expanding rapidly,
- digital dependence is increasing,
- and security threats are becoming more complex.

Thus, disaster management is gradually shifting from reactive relief-based approaches toward proactive risk reduction and early warning systems.



b. Understanding Cell Broadcast Technology

Meaning of Cell Broadcast Technology

Cell Broadcast Technology is a communication system through which emergency alerts are simultaneously transmitted to all mobile phones connected to a specific telecom tower or group of towers.

Unlike ordinary SMS systems, where messages are sent individually to each user, cell broadcast functions through a one-to-many transmission model.

In simple terms, it works like a radio announcement transmitted directly through mobile towers.

Thus, one emergency message can instantly reach lakhs of people located within a particular geographical area.

Basic Working Mechanism

Mobile phones constantly remain connected to nearby telecom towers for normal communication services.

The government can use this existing telecom infrastructure to transmit emergency alerts directly through these towers.

The process works in the following stages:

Step	Function
Step 1	Government agency generates emergency alert
Step 2	Alert transmitted to telecom operators
Step 3	Telecom towers broadcast warning signal
Step 4	All nearby mobile phones receive alert simultaneously

One major advantage is that the system continues functioning even during:

- heavy network congestion,
- excessive call traffic,
- or partial communication breakdown caused by disasters.

This makes it more reliable than ordinary SMS systems during emergencies.

c. Key Features of the Cell Broadcast System

Instant Mass Communication

One of the biggest strengths of cell broadcast technology is speed.

Since the system broadcasts one common signal rather than sending separate messages individually, alerts can reach millions of users within seconds.

This becomes especially important during sudden disasters such as:

- earthquakes,
- flash floods,
- industrial explosions,
- or tsunami warnings.

Rapid communication improves survival chances significantly.

Location-Based Targeting

The technology allows highly precise geographic targeting.

Alerts can be limited only to affected regions rather than being transmitted nationwide.

For example:

- cyclone warnings may target coastal districts,
- flood alerts may focus on river-basin regions,
- and earthquake warnings may cover affected seismic zones.

This reduces unnecessary panic and improves administrative efficiency.

Multilingual Communication

India's linguistic diversity makes multilingual alerts extremely important.

The system can transmit warnings in:

- English,
- Hindi,
- and regional languages.

In future, alerts may also support foreign languages for tourists where technical support exists.

This improves inclusiveness and ensures that local populations clearly understand emergency instructions.

Highly Noticeable Alerts

Unlike ordinary text messages, emergency alerts are specifically designed to immediately attract public attention.

The alerts:

- override mobile screens,
- produce loud warning sounds,
- generate strong vibrations,
- appear even during active calls,
- and function despite silent or Do-Not-Disturb modes.

This ensures that warnings are difficult to ignore during emergencies.

No Internet Requirement

The technology works without:

- mobile internet,
- Wi-Fi,
- or separate mobile applications.

Only a switched-on mobile phone connected to a telecom tower is required.

This is especially important in:

- rural regions,
- disaster-hit zones,
- and low-connectivity areas.

Privacy-Friendly System

One important feature of cell broadcast technology is that it does not rely upon personal user data.

The system does not require:

- phone numbers,
- identity details,
- or individual location tracking.

Instead, alerts are transmitted anonymously to all devices connected to a specific telecom tower.

Thus, the technology balances:

- public safety,
- rapid communication,
- and privacy protection.

d. Difference Between SMS Alerts and Cell Broadcast

Aspect	SMS Alerts	Cell Broadcast
Delivery mechanism	Individual messaging	One-to-many broadcasting
Speed	Slower during congestion	Extremely fast
Network load	High	Very low
Visibility	Easily ignored	Loud and prominent
Geographic precision	Limited	Highly precise
Internet requirement	Not required	Not required
Privacy concerns	Uses phone numbers	Anonymous transmission

This comparison explains why many countries are gradually shifting from conventional SMS-based warning systems toward broadcast-based emergency communication.

e. Why Cell Broadcast Technology is Important

i. Rising Climate Disasters

India is highly vulnerable to:

- cyclones,
- floods,
- heatwaves,
- cloudbursts,

- landslides,
- earthquakes,
- and extreme weather events.

Climate change is increasing both the frequency and intensity of disasters.

Early warning systems reduce casualties by giving citizens time to respond appropriately.

For example:

- evacuation before cyclones,
- movement to safer zones during floods,
- or protective action during heatwaves.

ii. Faster Disaster Response

Timely communication improves preparedness at both individual and institutional levels.

Citizens can:

- avoid dangerous travel,
- evacuate high-risk zones,
- store emergency supplies,
- and seek shelter quickly.

Simultaneously, government agencies gain additional time for rescue and coordination.

iii. Strengthening India's Disaster Management Framework

The system strengthens India's broader disaster preparedness architecture.

It supports institutions such as:

- National Disaster Management Authority (NDMA),
- State Disaster Management Authorities,
- India Meteorological Department (IMD),
- and emergency response agencies.

The system also aligns with the:

Sendai Framework for Disaster Risk Reduction

The Sendai Framework emphasises:

- early warning systems,
- disaster resilience,
- risk reduction,
- and preparedness-based governance.

iv. Utility for National Security

The technology is important not only for natural disasters but also for national security situations.

It may be used during:

- terror attacks,

- chemical leaks,
- industrial accidents,
- biological emergencies,
- border crises,
- or wartime situations.

Thus, the system has both humanitarian and strategic significance.

This growing importance of emergency alerts has encouraged several countries to develop advanced nationwide warning systems.

f. Global Adoption of Emergency Broadcast Systems

Many countries already operate similar public warning systems.

Country	System
Japan	Earthquake and tsunami alerts
United States	Wireless Emergency Alerts
South Korea	National disaster alerts
Singapore	Public warning framework
European Union	EU-Alert system

Japan's Example

Japan is considered one of the most advanced users of emergency broadcast systems because of its vulnerability to:

- earthquakes,
- tsunamis,
- and volcanic activity.

Its warning systems have repeatedly helped reduce casualties by providing citizens precious seconds or minutes for evacuation.

g. India's Institutional Framework

i. Development Agency

India's Cell Broadcast Emergency Alert System has been developed by:

Centre for Development of Telematics (C-DOT)

under the Department of Telecommunications (DoT)

ii. Coordinating Institutions

Implementation requires coordination among multiple agencies, including:

- NDMA,
- IMD,
- telecom operators,

- state disaster authorities,
- and emergency response agencies.

Such coordination is essential because disaster communication requires:

- real-time information sharing,
- rapid decision-making,
- and coordinated response mechanisms.

h. Challenges in Implementation

Device Compatibility

Some older mobile phones may not fully support advanced broadcast alerts.

This may reduce effectiveness in certain regions.

Public Awareness Deficit

Many citizens may:

- panic unnecessarily,
- misunderstand warnings,
- or ignore alerts completely.

Public education and awareness campaigns are therefore essential.

Risk of Alert Fatigue

Frequent testing or false alarms may reduce seriousness toward warnings.

This phenomenon is known as: “Alert Fatigue”

If people repeatedly receive non-serious alerts, they may stop responding during real emergencies.

Telecom Coordination Challenges

Effective functioning requires strong coordination among:

- government agencies,
- telecom companies,
- disaster authorities,
- and local administrations.

Technical failures or delays may reduce effectiveness.

Multilingual Accuracy

India’s linguistic diversity creates challenges regarding:

- accurate translation,
- region-specific instructions,
- and clarity of messaging.

Poorly translated warnings may create confusion during emergencies.

Rural Connectivity Gaps

Remote regions with weak telecom infrastructure may remain vulnerable.

This is especially relevant for:

- Himalayan regions,
- tribal areas,
- islands,
- and border districts.

These challenges highlight the need for long-term institutional strengthening and technological integration.

i. Way Forward

Nationwide Integration

India should ensure:

- full telecom integration,
- interoperability across operators,
- and universal geographic coverage.

Public Awareness Campaigns

Citizens should be educated regarding:

- meaning of alerts,
- evacuation behaviour,
- emergency preparedness,
- and official response procedures.

Prepared populations respond more effectively during disasters.

Integration with Forecasting Systems

The system should directly integrate with:

- IMD forecasting systems,
- flood monitoring networks,
- seismic monitoring systems,
- and industrial safety mechanisms.

This can enable automated real-time warning systems.

Regular Mock Drills

Periodic testing improves:

- public confidence,
- institutional preparedness,
- and inter-agency coordination.

Mock drills also help identify technical weaknesses.

Strengthening Last-Mile Connectivity

Special attention must be given to vulnerable and remote areas where communication infrastructure remains weak.

India should strengthen:

- resilient telecom networks,
- satellite-supported communication,
- and emergency backup systems.

This ensures wider outreach during disasters.

j. Broader Strategic Significance

India's Cell Broadcast Emergency Alert System reflects an important transition from:

- reactive disaster response
  to
- proactive disaster preparedness.

The system demonstrates how technology is increasingly being used for:

- citizen safety,
- climate resilience,
- governance efficiency,
- public communication,
- and national preparedness.

In the coming decades, early warning systems will become central to:

- climate adaptation,
- urban resilience,
- disaster governance,
- and human security.

Countries with advanced emergency communication systems will be better prepared to manage large-scale crises.

Conclusion

India's Cell Broadcast Emergency Alert System represents a major step toward building a modern, technology-driven disaster management framework.

The system combines:

- rapid communication,
- geographic precision,
- multilingual outreach,
- privacy protection,
- and large-scale public connectivity.

In an era of increasing climate disasters, urban vulnerabilities, and security challenges, timely communication can save thousands of lives.

If implemented effectively, the technology can become a cornerstone of India's disaster preparedness architecture, strengthening not only emergency response capacity but also long-term national resilience, public safety, and climate adaptability.

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.