# Prahaar – India's First Comprehensive Counter-Terror Doctrine

**Mains:** *GS III – Internal Security*

## Why in News?

*Recently, India has unveiled its first-ever comprehensive counter-terrorism doctrine titled* ***'Prahaar'****, marking a significant evolution in the country's security architecture.*

## What is the rationale behind the policy?

- **Persistent Cross-Border Terrorism**
  - Continued threats from hostile neighbours allegedly using terrorism as an instrument of state policy.
  - Presence of jihadi outfits and global terror networks such as ISIS and Al-Qaeda.
- **Evolving Nature of Terrorism**
  - Use of modern technologies including drones, encrypted messaging apps, dark web, and cryptocurrency.
  - Increasing nexus between terrorist organisations and organised criminal networks.
- **Need for Institutional Coordination**
  - Multiplicity of agencies dealing with terrorism necessitated a unified doctrine.
  - Requirement for synergy among central, state, and district-level authorities.



**STRESS ON DISRUPTING TERROR FUNDS**

- Special emphasis given to disrupting terror funding networks 'through **legal framework under Indian laws'**
- **Response to terror attack a multi-stakeholder exercise** involving agencies at central, state and district levels, with an SOP issued by MHA
- Indian laws, including anti-terrorism laws, '**give due importance to human rights'**. India adheres to rule of law 'where laws are just, applied evenly and protect fundamental rights'
- Extremists based on foreign soil **using the latest tech,** including drones, to **unleash terror in Punjab and J&K**
- **Poverty and unemployment** among vulnerable sections addressed through govt schemes to **prevent inimical elements from exploiting these conditions**

## What are the key features of ‘prahaar’ doctrine?

> ***‘Prahaar’*** *is an acronym representing seven pillars of India’s counter-terror strategy*

- **Prevention**
  - Focus on intelligence-based preventive action.
  - Early detection of radicalisation trends.
  - Strengthening surveillance and monitoring mechanisms.
- **Response**
  - Swift and proportionate retaliation to terror attacks.
  - Graded police response depending on the level of radicalisation.
  - Uniform anti-terror structures and Standard Operating Procedures (SOPs) across jurisdictions.
- **Aggregation of Capacities**
  - Whole-of-government approach integrating intelligence, law enforcement, and security agencies.
  - Modernisation of LEAs with advanced tools, technology, and weaponry.
  - Enhanced collaboration in intelligence collection and investigation.
- **Human Rights and Rule of Law**
  - Legal processes ensuring safeguards and avenues of appeal for accused persons.
  - Emphasis on balancing national security with constitutional values.
- **Attenuation of Enabling Conditions**
  - Addressing socio-economic vulnerabilities that lead to radicalisation.
  - Education, constructive engagement, and de-radicalisation programmes.
  - Disrupting overground worker networks and recruitment pipelines.
- **Alignment with International Efforts**
  - Cooperation through extradition, deportation, and adherence to UN norms.
  - Global partnerships to counter misuse of ICT by terrorist groups.
  - Investments in technological cooperation and private-sector collaboration.
- **Recovery**
  - Whole-of-society approach for post-attack rehabilitation and resilience building.
  - Strengthening community engagement to restore normalcy.

## What are the emerging threat dimensions highlighted?

- **Cyber and Technological Threats**
  - Use of encrypted platforms, dark web, and crypto for anonymity.
  - Proactive disruption of cyber activities of terror groups.
- **Drone and Hybrid Warfare**
  - Deployment of drones for cross-border smuggling of arms and narcotics.
- **Criminal-Terror Nexus**
  - Use of organised crime networks for logistics, financing, and recruitment.
- **Transnational Collaboration**
  - Foreign-based terror groups leveraging local infrastructure and terrain knowledge.

## What are the significance of the policy?

- **Doctrinal Clarity –** Elevates counter-terrorism from an operational strategy to a formal doctrine.
- **Institutional Uniformity –** Standardised structures and processes across levels of governance.
- **Holistic Approach –** Integrates security, socio-economic, legal, and international dimensions.
- **Balancing Security and Rights –** Acknowledges the importance of human rights in counter-terror operations.

## What are the challenges?

- **Federal Coordination Issues –** Policing is a State subject and hence ensuring uniform adoption may be complex.
- **Technological Upgradation –** Continuous investment required to match evolving cyber threats.
- **Capacity Building –** Need for trained manpower and specialised investigation skills at the state level.
- **Preventing Misuse –** Safeguards must prevent overreach and protect civil liberties.
- **International Cooperation –** Effective enforcement of extradition and global cyber norms requires diplomatic agility.

## What lies ahead?

- The unveiling of ‘Prahaar’ marks a significant milestone in India’s internal security framework.
- By institutionalising a proactive, intelligence-driven and coordinated approach, the policy seeks to address both conventional and emerging dimensions of terrorism.
- Its success, however, will depend on effective federal cooperation, technological preparedness, safeguarding civil liberties, and sustained international collaboration.
- If implemented robustly, Prahaar could strengthen India’s resilience against the evolving threat of terrorism while upholding democratic values.

## Reference

The Times of India| Prahaar

SHANKAR IAS PARLIAMENT
Information is Empowering