ujiyari

UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

DAILY CURRENT AFFAIRS

Prahaar — India's First Comprehensive Counter-Terrorism Policy Framework

23 February 2026

SUBJECTS COVERED

SECURITY & DEFENCE POLITY

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator •
linkedin.com/in/epicbharat

Prahaar — India's First Comprehensive Counter-Terrorism Policy Framework

23 February 2026 ·

WHY IN NEWS

The Ministry of Home Affairs released "Prahaar" — India's first-ever comprehensive counter-terrorism policy framework — covering prevention and response across land, air, and maritime domains, with specific focus on drone threats, cyber attacks on critical infrastructure, CBRN risks, and digital financing of terrorism.

WHAT IS PRAHAAR?

Prahaar (meaning "strike" in Sanskrit) is India's **first comprehensive national counter-terrorism policy framework**, released by the **Ministry of Home Affairs (MHA)**. The framework marks a qualitative shift from ad hoc responses to individual incidents toward a systematic, whole-of-government approach to countering terrorism in all its forms.

The policy covers three operational domains:

Land: Cross-border terrorism, especially from India's western frontiers (Pakistan and its proxy networks)

Air: Drone-based smuggling and potential aerial attacks — particularly in Punjab and Jammu & Kashmir

Maritime: Coastal terrorist infiltration and sea-borne threats (context: 26/11 Mumbai attacks used maritime routes)

THREAT ASSESSMENT — WHAT PRAHAAR IDENTIFIES

CROSS-BORDER TERRORISM AND PROXY WARFARE

The framework identifies **organised cross-border terrorism from India's western frontiers** as the primary conventional threat — referring primarily to Pakistan-based terror groups operating in Jammu & Kashmir and Punjab. It emphasises that terror networks increasingly use **civilian cover** and exploit legal grey areas to evade prosecution.

DRONE-BASED THREATS

A significant new dimension: **drones are now used systematically to smuggle arms, narcotics, and counterfeit currency** into Punjab and J&K from across the international border. Post-2021, there have been hundreds of documented drone incidents. Prahaar mandates:

- Integrated counter-drone systems at vulnerable borders
- Legal framework for detecting, intercepting, and destroying hostile drones
- Coordination between BSF, CRPF, state police, and DRDO (which has developed the D4 counter-drone system)

CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Prahaar designates **nine categories of critical infrastructure** as priority protection targets: power grids, railways, aviation, ports, defence establishments, space assets, atomic energy facilities, financial systems, and telecommunications networks.

The framework calls for mandatory vulnerability audits, incident response protocols, and information-sharing between CERT-In (Computer Emergency Response Team), NCIIPC (National Critical Information Infrastructure Protection Centre), and sector regulators.

CBRN THREATS

Chemical, Biological, Radiological, and Nuclear (CBRN) threats from non-state actors are addressed — including the risk of radiological dirty bombs, bioterrorism using pathogens, and chemical agent deployment. Prahaar mandates inter-agency CBRN response drills and coordination with the Department of Atomic Energy (DAE) and DRDO's CBRN division.

DIGITAL TERRORISM FINANCING

Dark web recruitment and cryptocurrency-based terror financing are explicitly addressed — an acknowledgment that the terror financing landscape has moved well beyond hawala networks. Prahaar calls for:

- Financial Intelligence Unit (FIU-IND) to enhance crypto transaction monitoring
- Coordination with the Enforcement Directorate (ED) for PMLA enforcement against terror proceeds
- Legislative amendments to bring virtual digital assets under UAPA's definition of terror financing

INSTITUTIONAL RESPONSE ARCHITECTURE

NIA — STRENGTHENED MANDATE

The **National Investigation Agency (NIA)**, established under the NIA Act 2008 following the 26/11 Mumbai attacks, is designated as the primary federal counter-terrorism investigation agency. Prahaar mandates **legal experts integrated throughout investigation and prosecution** — addressing the historically low conviction rate in terror cases (often below 30%).

DE-RADICALISATION FRAMEWORK

A comprehensive **de-radicalisation** component is new to the policy:

Programme	Target	Mechanism
Youth Prevention	Vulnerable youth	Community engagement, religious leaders, NGOs
Prison De-radicalisation	Convicted terrorists	Psychological counselling, religious education, skill training
Family Engagement	Families of radicalised individuals	Early-warning networks, welfare support
Social Media Monitoring	Online radicalisation	CERT-In, NIA, state police coordination

INTERNATIONAL INTELLIGENCE SHARING

Prahaar formalises enhanced intelligence-sharing with bilateral partners — building on India's existing mechanisms under SAARC agreements, bilateral MoUs (India has counter-terrorism MoUs with over 40 countries), and multilateral bodies including the **Financial Action Task Force (FATF)** and the **Shanghai Cooperation Organisation (SCO)** counter-terrorism structure.

LEGAL ARCHITECTURE FOR COUNTER-TERRORISM IN INDIA

India's counter-terrorism legal framework includes several statutes:

Law	Key Provisions
UAPA 1967 (amended 2004, 2008, 2019)	Designates terrorist organisations + individuals; enables preventive detention; NIA investigates
NIA Act 2008	Establishes NIA; concurrent jurisdiction to investigate specified offences
PMLA 2002 (amended 2019)	Criminalises money laundering including terror financing
IT Act 2000 (amended 2008)	Covers cyber terrorism (Section 66F — up to life imprisonment)
NDPS Act 1985	Narcotics trade funding terror networks

Prahaar's call for legislative amendments to cover cryptocurrency is expected to modify UAPA's Section 2(1)(g) definition of "proceeds of terrorism."

UPSC RELEVANCE

Prahaar (MHA, India's first CT policy), NIA (NIA Act 2008), UAPA (1967, amended 2019), NCIIPC, CERT-In, FIU-IND, DRDO D4 counter-drone system, CBRN threats, FATF, SCO counter-terrorism, BSF, CRPF, Financial Intelligence Unit. **Mains GS-3:** *Internal security; counter-terrorism policy; cyber security; critical infrastructure protection; terror financing; Left Wing Extremism vs. Islamist terrorism policy distinction; role of technology in counter-terrorism.* **Interview:** *"India has had UAPA for nearly 60 years, and now a comprehensive CT policy. But critics argue these laws create a chilling effect on civil liberties without adequately addressing structural causes of radicalisation. How should India balance national security imperatives with fundamental rights under Article 19 and 21?"*

📌 FACTS CORNER — KNOWLEDGEPEDIA

PRAHAAR FRAMEWORK:

Released by: **Ministry of Home Affairs (MHA)**

India's **first comprehensive counter-terrorism policy**

Domains: Land, Air, Maritime

Key threat categories: Cross-border terrorism, drone smuggling (Punjab/J&K), cyber attacks on critical infrastructure, CBRN, dark web/crypto terror financing

KEY INSTITUTIONS:

NIA: National Investigation Agency | Established: NIA Act 2008 (after 26/11) | HQ: New Delhi

IB: Intelligence Bureau — domestic intelligence; established 1887; under MHA

RAW: Research and Analysis Wing — foreign intelligence; established 1968; under PMO

CERT-In: Computer Emergency Response Team India | Under MeitY | Handles cyber incidents

NCIIPC: National Critical Information Infrastructure Protection Centre | Under NTRO (PMO) | Protects critical info infrastructure

FIU-IND: Financial Intelligence Unit — India | Under Ministry of Finance | Monitors financial transactions for suspicious activity

UAPA (UNLAWFUL ACTIVITIES PREVENTION ACT):

Original: 1967 | Amended: 1986, 2004, 2008, **2019** (most significant)

2019 amendment: Allows designation of **individuals** as terrorists (previously only organisations)

Schedule 1: Listed terrorist organisations (Lashkar-e-Taiba, Jaish-e-Mohammed, ISIS etc.)

NIA + state police both investigate UAPA offences

COUNTER-DRONE SYSTEM:

DRDO developed **D4 system** (Detection, Deterrence, Disable, Destroy)

Also: CUAS (Counter Unmanned Aerial System) technology being deployed at borders

Legal basis for drone interception: Still evolving; UAS Rules 2021 under the Drone Rules 2021

FATF (FINANCIAL ACTION TASK FORCE):

Established: 1989 | HQ: Paris | Members: 37 + 2 regional organisations

India joined: 2010 | India's status: Currently in compliance (removed from enhanced monitoring)

Pakistan: Grey-listed 2018, delisted 2022

Evaluates anti-money laundering and counter-terrorism financing frameworks

OTHER RELEVANT FACTS:

26/11 Mumbai Attacks (Nov 26-29, 2008): LeT attackers arrived by sea; 166 killed → led to NIA formation, coastal security overhaul

CBRN threats: India has signed Chemical Weapons Convention (CWC), Biological Weapons Convention (BWC); DRDO has CBRN Defence Wing

SCO counter-terrorism: SCO-RATS (Regional Anti-Terrorist Structure) based in Tashkent; India joined SCO 2017

India's conviction rate in terror cases has historically been low — Prahaar addresses this through legal experts in prosecution teams

Sources: GKToday, The Hindu, PIB

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

Published on **ujiyari.com** · Free UPSC & State PCS Current Affairs