2. Anti-Terrorism Conference 2025- Internal Security

Amit Shah inaugurates Anti-Terrorism Conference 2025, calls for strong, unified national security grid. The union home minister inaugurated the Anti-Terrorism Conference-2025, culminating in India's first National Counter-Terrorism Policy, which aims to create an "impenetrable grid" by unifying state ATS structures and shifting from a "Need to Know" to a "Duty to Share" intelligence model. This policy addresses modern hybrid threats like digital radicalisation and cyber-terrorism through a proactive, technology-led doctrine anchored in recent legal reforms like the Bharatiya Nyaya Sanhita.

Overview

Event- The union home minister inaugurated the Anti-Terrorism Conference-2025 in New Delhi.
Organizer- The conference was organised by the National Investigation Agency (NIA).
Key Outcome- The deliberations culminated in the finalisation of India's first comprehensive National Counter Terrorism Policy and Strategy.

Key Highlights of the Anti-Terrorism Conference-2025

Impenetrable Anti-Terrorism Grid- The union home minister proposed the creation of a nationwide anti-terror architecture.
Goal- To establish an "impenetrable grid" that enhances India's capacity to tackle evolving terror threats.
Unified ATS Structure- There is a strong emphasis on standardizing the Anti-Terrorism Squad (ATS) structure across all states and Union Territories.
Benefits- This aims to improve coordination, remove operational silos between states, and ensure rapid response times during crises.
Intelligence Sharing Shift- The framework signals a fundamental shift in intelligence sharing protocols.
Transition- Moving from a restrictive "Need to Know" approach to a collaborative "Duty to Share" model among intelligence and enforcement agencies to speed up threat detection.
Digital Tools & Databases- Launch of critical tools to modernize counter-terror operations and strengthen data integration via platforms like NATGRID and NIDAAN.

New Launches

Updated NIA Crime Manual- To guide investigations and prosecutions.
Organised Crime Network Database- To track linkages between criminals and terrorists.
National Database of Lost, Looted & Recovered Weapons- To monitor illegal arms circulation.
360-Degree Strike on Organised Crime- Introduction of a holistic plan targeting organised crime networks that fund or support terrorism.
Method- Leveraging shared intelligence and digital databases for preemptive action.
Emerging Threats & Legal Measures- The conference focused on modern threats such as cyber threats, digital anonymity, deepfakes, hybrid warfare, and maritime terrorism. It also discussed evolving counter-terrorism laws to ensure swift legal action.
Lessons from Counter-Terror Operations- Cited specific intelligence-led operations like Operation Sindoor and Operation Mahadev as examples of decisive action taken against terror networks.
Radicalisation & Conviction Rates- Emphasized the need to tackle youth radicalisation. Stressed scaling up high conviction rates across police forces to strengthen internal security.

About the Anti-Terrorism Conference

Nature- It is an annual national-level conference organised by the NIA under the Ministry of Home Affairs.
Institutional Framework- It is a non-statutory, executive, and operational coordination platform.
Focus- It prioritizes strategic review, operational preparedness, and institutional coordination rather than legislative or judicial functions.
Composition- Participants include senior officers from central and state security agencies (NIA, IB, State Police, ATS, CAPFs).
Goal- To ensure inter-agency coordination and Centre–State operational convergence.

Objectives- Assess evolving threats like cross-border terrorism, the crime-terror nexus, and terror financing. Strengthen information sharing and investigative capacity. Reinforce India's zero-tolerance approach with an emphasis on prevention, disruption, and prosecution.

About India's First Anti-Terror Policy (2025)

Context- The policy is the culmination of two decades of institutional learning post-26/11.
Design- It is designed to shield India's economic progress as one of the world's largest economies.
Unified Doctrine- Consolidates central agencies and state police into a cohesive "Team India**"**. Aims to counter **hybrid terrorism** where physical and digital threats are linked.

Major "New-Age Terror Threats" Targeted

1. **Digital Radicalisation-** Addressing "white-collar radicalisation" where educated professionals are targeted via foreign-funded online modules and encrypted platforms.
2. **Open Border Vulnerabilities-** Tackling porous corridors (e.g., India–Nepal–Bihar route) used by insurgent groups with foreign passports.
3. **Aadhaar and Document Spoofing-** Targeting "ghost identities" created using forged documents to hide sleeper cells in urban areas.
4. **Information Warfare-** Countering the use of social media for disinformation and inciting communal disharmony.

No Anti-Terror Policy Until Now

Ad-hoc Measures- Historically, India relied on reactive legislative measures rather than a codified national doctrine.
Federal Friction- "Police" and "Public Order" are State subjects (7th Schedule), leading states to view central policies as "overreach."
Intelligence Silos- A "Need to Know" culture prevented the creation of a Unified Intelligence Architecture.
Reactive vs. Proactive- Previous laws (UAPA, POTA) were largely punitive (post-event), whereas a policy is preventative (pre-event).
Definitional Ambiguity- Difficulty in balancing definitions of insurgency, militancy, and terrorism led to fragmented legal responses.

Need for a National Counter-Terror Policy

Rise of Hybrid Terrorism- Groups now combine local modules with high-end tech (drones, encrypted apps), bypassing traditional boundaries (e.g., Pahalgam attack, April 2025).
Narco-Terror Nexus- Approximately 30% of terror financing in border states is linked to international drug cartels.
Digital Radicalisation- Increasing targeting of educated youth requires advanced Cyber-Human Intelligence (CHINT) capabilities.
Changing Landscape- While mass-casualty attacks have declined, hybrid threats (cyber recruitment, transnational networks) are rising (India ranks 14th on Global Terrorism Index 2025).
Systemic Weaknesses- Despite post-26/11 gains, structural gaps persist, and conviction rates under UAPA remain low (around 3%) due to poor investigation and forensic capacity.

India's Contemporary Counter-Terrorism Framework

The following table differentiates the legal, institutional, and strategic components of India's current framework.

Dimension	Key Components	Core Features / Significance
Legal Framework	Unlawful Activities (Prevention) Act, 1967	Enables designation of terrorists, asset attachment, and extended investigation periods (up to 180 days).
	National Investigation Agency Act, 2008	Grants' NIA nationwide jurisdiction to investigate terror offences without prior State consent.
	National Security Act, 1980	Provides for preventive detention to neutralise threats to national security.

	Bharatiya Nyaya Sanhita, 2024 (Section 113)	Introduces a modernised definition of "terrorist act", bridging gaps between local policing and central inputs.
Institutional Architecture	National Investigation Agency (NIA)	Principal federal counter-terror prosecution agency.
	National Intelligence Grid (NATGRID)	Technology-driven intelligence fusion platform integrating banking, travel, and telecom data.
	Specialised Units (NSG & State ATS)	Primary tactical response forces for urban incidents and hostage rescue.
	National Security Council Secretariat (NSCS)	Headed by the NSA, ensuring whole-of-government coordination.
Strategic Doctrine	Strategic Autonomy	Treats terror attacks as serious national security violations allowing flexible response.
	Sponsor Accountability	Holds state sponsors equally responsible alongside terror groups.
	Punitive Deterrence	Shifts from deterrence by denial to deterrence by punishment.

Constitutional, Legal, and Judicial Anchoring

Constitutional Mandate

Article 355- The Union has the duty to protect states against "internal disturbance."

Cooperative Federalism- While policing is a state subject, the policy promotes a Common ATS Structure for operational uniformity.

Judicial Alignment- The policy integrates with Section 113 of the Bharatiya Nyaya Sanhita (BNS) for a modern definition of terrorism. Ensures data processing via NATGRID/NIDAAN aligns with the K.S. Puttaswamy (Privacy) judgment.

Trial in Absentia- Section 356 of Bharatiya Nagarik Suraksha Sanhita (BNSS) allows for the trial of proclaimed offenders in their absence. This is intended to compel fugitives to return, subject to natural justice and international laws.

Way Forward

Incentivised Federalism- The Union Government should introduce conditional internal security grants to encourage states to adopt the unified ATS structure and updated manuals.

Strengthened Institutional Coordination- Use platforms like the Inter-State Council and National Conference of Chief Secretaries to resolve data-sharing frictions and build trust.

Integrated Soft-Power Strategy- Combine hard-power operations with community policing and capacity building to detect early signs of digital radicalisation.

Conclusion

The Anti-Terrorism Conference-2025 and the new National Counter-Terrorism Policy mark a transition from reactive policing to a proactive, technology-led doctrine. By institutionalizing a unified ATS structure and a "Duty to Share" intelligence model, the framework aims to create an impenetrable security grid essential for the stability of Viksit Bharat 2047.

Source- https-//ddnews.gov.in/en/amit-shah-inaugurates-anti-terrorism-conference-2025-calls-for-strong-unified-national-security-grid/