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: November 2025

Printed and published by PrepAlpine

Why This Book

UPSC preparation today suffers from an irony: aspirants have access to *more material than ever before*, yet they struggle to find material that genuinely improves their marks.

The ecosystem is flooded with bulky PDFs, poorly curated compilations, and recycled coaching notes. They provide information, not intelligence; volume, not value. When aspirants finally sit down to write answers, these resources fail them — lacking depth, structure, contemporary linkage, and exam usability. Months of effort dissolve into generic, forgettable responses.

This book was created to solve that exact problem — by setting a new benchmark for what a UPSC book should be in 2025 and beyond.

Rather than adding another document to your already-cluttered folder, we designed this book around *10 objective parameters* that define high-quality UPSC content. Every chapter has been built to meet — and exceed — these standards:

1. Complete & Precise Syllabus Coverage

Every topic is mapped line-by-line to the official syllabus and extended to include emerging themes UPSC increasingly tests — ensuring you never miss conceptual blind spots.

2. Depth with Analytical Rigor

Concepts are not stated — they are explained, contextualized, and analysed. You learn the *why*, *how*, and *so what*, not just the *what*.

3. Real-World Examples & Case Studies

From landmark judgments to NCRB trends, World Bank insights to policy best practices — this book integrates authenticity that elevates answers instantly.

4. Static–Dynamic Fusion

Every static idea is tied to current affairs seamlessly. UPSC doesn't ask siloed questions anymore — and neither should your notes.

5. Visual Pedagogy as a Core Feature

Flowcharts, diagrams, tables, and infographics simplify complexity, accelerate revision, and boost recall under exam pressure.

6. Clear, Scholarly Language

The writing is precise, readable, and exam-oriented — free from clutter, jargon, or casual tone. Every sentence pulls its weight.

7. Seamless Flow & Conceptual Continuity

Chapters are stitched together with bridging paragraphs that help you see the bigger picture — how ideas evolve, connect, and reinforce each other.

8. Aesthetic, Revision-Friendly Design

Professional layout, spacing, highlighting, and formatting make long-hour study easier, faster, and more effective.

9. Exam Readiness in Every Page

IBC structure, directive-word cues, answer frameworks, and value-add points make this not just a book but an answer-writing engine.

10. Updated, Authenticated & Reliable Sources

Every chapter incorporates the latest data, schemes, policies, and global reports — with zero outdated clutter.

The Core Idea

This book is not meant to be *read* and forgotten; it is meant to be *used* — as a high-precision instrument that converts knowledge into marks.
It combines research, rigor, integration, visual learning, and exam-ready design into one ecosystem.

Welcome to PrepAlpine — where preparation becomes intelligent, integrated, and truly exam-worthy.

Table of Contents

Chapter 1. Conceptual Framework

1.1 Definition and Scope of Internal Security

a. Introduction

Internal security may be defined as the comprehensive safeguarding of a nation's internal order, legitimacy, and cohesion from threats that arise within its borders, or through actors embedded inside the country but supported externally. It extends far beyond the physical protection of life and property, reaching into the defence of constitutional values, socio-political harmony, and the larger project of national integration.

The scope of internal security is wide and multidimensional. It involves:

- Maintaining public order and the rule of law,
- Protecting citizens from terrorism, insurgency, radicalisation, organised crime, cyber threats, and
- Preserving the unity and integrity of the nation against secessionist or communal forces.

In essence, internal security acts as the invisible shield that allows democracy to function, citizens to live without fear, and institutions to operate with authority and stability.

Unlike external aggression, which is more visible and military in nature, internal security threats are often diffuse, embedded within the social fabric, and constantly evolving with political, technological, and ideological changes. They may not always march under a banner or wear a uniform, yet their effects can be equally destabilising—if not more insidious.

As Kofi Annan aptly observed: *"Security is not just the absence of violence. It is the presence of justice, stability, and freedom from fear."* This highlights that internal security is not merely about neutralising threats but also about building inclusive and just societies.

b. Components of Internal Security

The domain of internal security spans across several interlinked dimensions. Each reflects a different facet of vulnerability and protection:

- **Political Security** – Safeguarding the state from insurgency, separatist movements, communalism, and extremist or hate-driven ideologies.
- **Economic Security** – Preventing illicit financial flows, including money laundering, terror financing, circulation of counterfeit currency, and large-scale cyber theft that can destabilise economic systems.
- **Societal Security** – Containing caste-based and religious violence, curbing radicalisation, and managing demographic tensions that can fracture the social fabric.
- **Technological Security** – Protecting critical information infrastructure against cyber intrusions, digital sabotage, and manipulation of public opinion through artificial intelligence–generated disinformation.

- **Environmental and Biosecurity** – Addressing internal displacement caused by ecological stresses, combating pandemics, and preparing against the risks of bio-attacks or engineered pathogens.

Together, these components constitute the architecture of a nation's internal resilience. Their interplay demonstrates that security is not merely a matter of force but also of governance, foresight, and societal trust.

c. Key Features of Internal Security in India

India's internal security landscape has distinct characteristics shaped by its geography, diversity, and federal governance structure. Some defining features are as follows:

i. **Territorial Focus** – Internal security is primarily concerned with threats that originate within India's territorial boundaries, although these are often entangled with transnational linkages such as cross-border financing, ideological support, or external instigation. For example, a terror attack in Jammu and Kashmir may be carried out by a local youth, but the module could have received training in Pakistan and financial support through hawala networks operating from Gulf countries.

ii. **Nature of Actors Involved** – The sources of internal threats are highly diverse: insurgent groups, separatist elements, radicalised individuals, organised crime syndicates, or even disaffected citizens. In contemporary contexts, the lines between internal and external actors have blurred. External state or non-state entities frequently operate through internal proxies, leveraging local vulnerabilities. Maoist cadres trained in remote forest camps represent a largely domestic threat, whereas Pakistan's ISI using local youth to trigger communal riots illustrates external manipulation through internal channels.

iii. **Primary Objectives of Internal Security** – The overarching aim is to preserve peaceful coexistence, uphold the rule of law, and safeguard institutional stability. This is achieved by preventing terrorism, political violence, ethnic or communal riots, radicalisation, law and order breakdowns, and internal sabotage. Thus, internal security acts as a vital safeguard for India's pluralistic democracy and its socio-economic development.

iv. **Agencies Involved** – Internal security in India is ensured through a multi-tiered apparatus:

- **Local Police** – First responders to incidents.
- **Central Armed Police Forces (CAPFs):** CRPF, BSF, CISF, ITBP, and SSB, tasked with riot control, border management, and Left Wing Extremism operations.
- **Intelligence Agencies:** IB (domestic intelligence), R&AW (external intelligence), and NIA (terror investigations).
- **Policy Coordination:** Ministry of Home Affairs oversees and coordinates efforts.

The effectiveness of internal security depends on seamless cooperation among these entities. The difference between pre-empting an attack and reacting after damage often lies in timely intelligence and coordination.

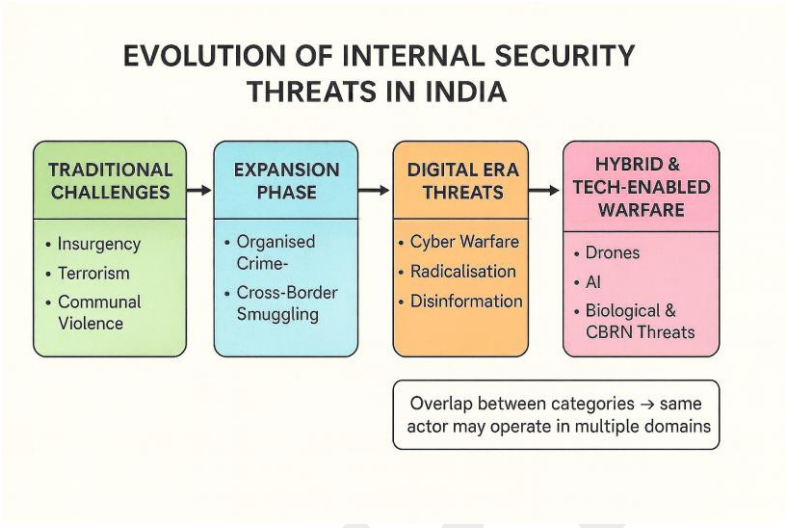
v. **Legal and Regulatory Support** – Internal security operations are empowered by a wide range of legal instruments:

- **Counter-terror and public order laws:** Unlawful Activities (Prevention) Act (1967), Armed Forces Special Powers Act (1958).
- **General law framework:** Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita.
- **Cybersecurity law:** Information Technology Act (2000).
- **Financial and organised crime laws:** Prevention of Money Laundering Act, Narcotic Drugs and Psychotropic Substances Act, Maharashtra Control of Organised Crime Act, National Security Act.

While essential, these laws are frequently scrutinised for the delicate balance they must maintain between security imperatives and civil liberties.

d. Scope of Internal Security

Internal security in India refers to the preservation of peace, public order, and constitutional governance against threats that arise domestically or are externally supported. Its scope has significantly expanded over time. Earlier it focused on insurgency, terrorism, and communal violence. Today, new-age threats such as cyber warfare, radicalisation via digital platforms, drone intrusions, and hybrid warfare have widened its ambit.



These threats are multidimensional, involving both state and non-state actors, and frequently operate across borders, technologies, and identities. In a diverse and federal country like India, internal security requires not only robust policing and intelligence but also inclusive governance, strong legal safeguards, and constant technological preparedness.

The scope may broadly be divided into three domains:

i. **Traditional Threats** – Insurgency in the North-East, terrorism (e.g., Pulwama attack 2019), Left-Wing Extremism (e.g., Sukma ambush 2021), and communal or regional unrest (e.g., Delhi riots 2020).

ii. **Organised Crime** – Criminal syndicates engaging in drug trafficking, human trafficking, arms smuggling, and counterfeit currency circulation. These activities often serve as funding channels for terrorism while weakening economic stability.

iii. **New-Age and Non-Traditional Threats** –

- **Cyberattacks:** e.g., ransomware attack on AIIMS (2022).
- **Espionage and surveillance:** e.g., Pegasus spyware.
- **Radicalisation through digital platforms, fake news, and disinformation.**
- **Drone-enabled attacks:** e.g., tiffin bomb in Punjab (2021).
- **Biological and chemical threats:** pandemics and CBRN hazards.
- **Hybrid warfare:** blending cyber operations, information warfare, and economic coercion.

Having examined the definition, components, features, and scope of internal security in India, it becomes evident that the subject is not merely theoretical but deeply rooted in lived realities. The vast canvas of threats—ranging from insurgency and terrorism to cyber warfare and hybrid attacks—shows that security is multidimensional and ever-expanding. Yet, recognition of the scope is only the first step. The real test lies in how effectively the state anticipates, manages, and neutralises these dangers. This sets the stage for an exploration of the challenges that complicate internal security management in India.

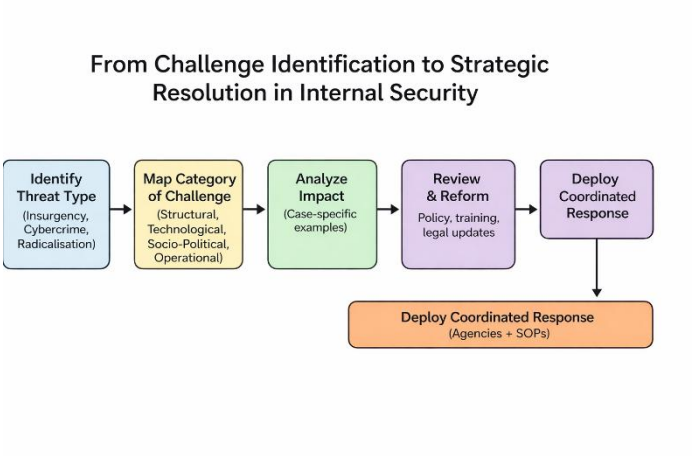
1.2 Challenges in Ensuring Internal Security in India

a. Introduction

India's internal security landscape is marked by complexity and constant evolution, shaped by its vast geography, diverse society, and sensitive regional environment. The range of threats has become

multidimensional—stretching from insurgency, terrorism, and communal violence to newer challenges such as cybercrime, radicalisation, drone intrusions, and hybrid warfare.

At the same time, weak inter-agency coordination, outdated infrastructure, and gaps in the legal framework constrain effective responses. Meeting these challenges requires a calibrated approach that combines structural reform, technological modernisation, and socio-political resilience.



i. Structural and Institutional Challenges

- **Centre–State Division of Responsibility** – Law and order is a state subject, but threats such as terrorism and Left-Wing Extremism have national implications. Lack of synergy between Union and state authorities often delays coordinated action. Delayed responses to cross-border terror incidents illustrate this weakness.
- **Fragmented Intelligence Sharing** – Agencies such as the IB, R&AW, NIA, and state intelligence units often function in silos. The 26/11 Mumbai terror attacks revealed this weakness: fragments of intelligence existed but were never pieced together in time.
- **Police Reforms Pending** – A colonial policing mindset, political interference in postings, inadequate modern training, and the absence of effective community policing continue to weaken law enforcement. Despite Supreme Court directives in the *Prakash Singh* case, most reforms remain unimplemented.

ii. Technological and Legal Challenges

- **Encrypted Communication and Dark Web** – The increasing use of encrypted platforms like Telegram, Signal, and the TOR network allows terrorists, drug syndicates, and radicalised youth to evade tracking. Several ISIS-inspired modules in India have exploited these channels.
- **Weak Cyber Forensics Capacity** – India faces a shortage of well-equipped laboratories and trained personnel. The 2022 ransomware attack on AIIMS illustrated this gap, with recovery efforts stretching over weeks.
- **Tensions in Legal Frameworks** – While laws such as the UAPA and NSA are essential to address grave threats, their frequent misuse raises concerns over liberty and due process. Prolonged denial of bail in UAPA cases, even when trials are delayed, exemplifies this tension.

iii. Socio-Political and Strategic Challenges

- **Radicalisation via Social Media** – The rapid spread of extremist ideologies, hate speech, and misinformation through online platforms has amplified social tensions. The Delhi riots of 2020 were reportedly fuelled by communal propaganda circulated digitally.
- **Ethnic and Communal Tensions** – Historical and political fault lines continue to erupt into violence. The Manipur conflict of 2023 and protests over the NRC in Assam reveal the fragility of such situations.
- **Border Management Vulnerabilities** – India's porous frontiers facilitate smuggling, infiltration, and arms transfers. Drone drops of weapons in Punjab and the infiltration of Rohingya refugees across the Bangladesh border highlight these persistent threats.

iv. Operational Challenges

- **Overstretched Security Forces** – CAPFs face a chronic burden, tasked with counterinsurgency, riot control, VIP protection, and election duties, often without adequate rotation.
- **Underutilisation of Technology** – Despite repeated drone incursions in Punjab, the absence of effective jammers reflects a lag in adopting modern tools. Predictive policing and AI-driven surveillance remain underdeveloped.
- **Judicial Delays** – Terror-related trials under UAPA or NSA frequently drag on for years. Many NIA cases have been pending for over a decade, undermining deterrence.
- **Inadequate Training for Urban Warfare** – The 26/11 Mumbai attacks exposed the lack of preparedness for urban combat. Similarly, India lacks standard operating procedures for new-age threats like lone-wolf attacks, drone strikes, or coordinated misinformation campaigns.
- **Shortage of Skilled Manpower** – Many law enforcement personnel lack expertise in cybercrime investigation, encryption tracking, and digital forensics. Even minor cases often require outsourcing to private labs due to inadequate in-house capacity.

Conclusion

Ensuring internal security in today's India demands more than the mere deployment of force. It requires a strategic blend of technology, justice, and coordination. The focus must shift from reactive policing to a proactive, intelligence-driven, and rights-respecting framework. Only through modernisation, institutional synergy, and the rebuilding of community trust can internal security become both effective and democratic.

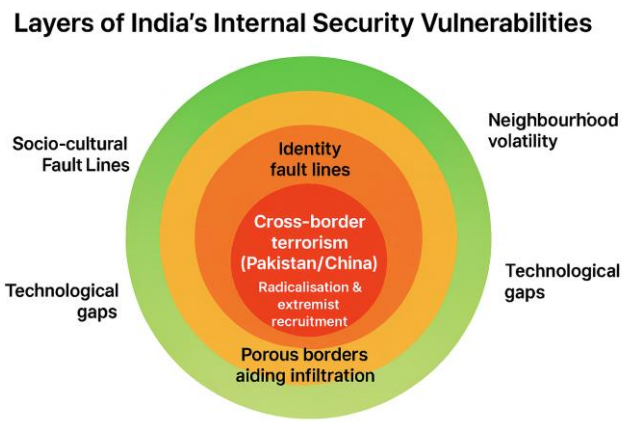
As K. Subrahmanyam, one of India's foremost strategic thinkers, observed: *"Internal security is not merely the absence of violence; it is the presence of justice, equity, and trust in the system."*

While many internal security challenges are common to modern states, India's situation carries distinct complexities rooted in its geography, demography, and historical experience. The multiplicity of borders, varied ethnic and religious identities, and the interplay of regional aspirations with national integration create a landscape unlike that of most countries. Beyond structural, technological, socio-political, and operational hurdles, India faces challenges that are uniquely tied to its national circumstances—making internal security management both exceptionally demanding and distinctively Indian.

Having assessed the challenges that complicate internal security, the next step is to explore the institutional mechanisms and policy responses India has evolved to deal with these threats. This will show how the state attempts to translate strategy into practice while navigating the tensions between liberty and security.

1.3 Challenges Unique to Internal Security in India

a. Introduction



India's internal security vulnerabilities are shaped by a complex socio-political fabric, vast geography, and a volatile regional environment. Unlike many other democracies, India must simultaneously manage deep identity fault lines, porous borders, asymmetric threats from adversarial neighbours, rapid grassroots technological penetration, and the operational constraints of constitutional federalism.

These challenges cut across multiple domains—counter-terrorism, anti–

money laundering, cybercrime prevention, border management, and the fight against organised crime—making them foundational to every dimension of India's internal security.

i. Socio-Cultural Diversity and Identity Fault Lines

- India's immense diversity of caste, religion, language, ethnicity, and region is a source of cultural strength but also a potential trigger of conflict.
- Divisive forces exploit these differences, fuelling communal polarisation, separatist mobilisations, and radicalisation.
- The Manipur violence (2023) highlighted the volatility of ethnic tensions, while the revival of Khalistani rhetoric—amplified through diaspora networks—demonstrates how identity politics can transcend borders and re-enter the domestic arena.

ii. Vast, Porous, and Inhospitable Borders

- India shares over 15,000 km of land borders and more than 7,500 km of coastline, much of which is forested, mountainous, riverine, or maritime—making regulation extremely difficult.
- Illegal migration, arms and drug smuggling, and infiltration are persistent concerns:
    - The Bangladesh border is used for illegal migration and cattle smuggling.
    - The Myanmar frontier sees narcotics and arms flows.
    - The Line of Control in Jammu & Kashmir is a hotspot for infiltration.

iii. Hostile and Volatile Neighbourhood

- India's internal vulnerabilities are inseparable from its external environment.
- Both Pakistan and China employ grey-zone tactics, proxy warfare, and cyber-espionage.
- Pakistan's ISI continues to back militant groups in Kashmir and Punjab, while China has been accused of cyber intrusions against India's power grid and critical infrastructure.
- Border incursions and covert support to separatist elements exacerbate internal insecurities.

iv. Technological Diffusion and Misuse

- The rapid penetration of affordable smartphones, cheap internet, and encrypted applications has transformed security challenges.
- Emerging technologies—deepfakes, drones, cryptocurrency, and the dark web—are increasingly exploited for radicalisation, illicit trade, and disinformation.
- Examples include:
    - ISIS-inspired online radicalisation in Kerala.
    - Drone drops of arms and counterfeit currency in Punjab.
    - Crypto-based money laundering networks that finance organised crime and extremism.

v. Federal Structure and Jurisdictional Constraints

- The constitutional division of powers complicates security management. "Police" and "public order" fall under the State List, creating fragmented authority.
- Coordination gaps and uneven state capacities weaken national responses.
- Jurisdictional disputes, such as resistance to the NIA or ED's interventions, exemplify these tensions.
- Counter-radicalisation programmes often vary across states, reducing their consistency and effectiveness.

vi. Coastal and Maritime Security Gaps

- India's long coastline, island territories, and unregulated fishing fleets pose persistent vulnerabilities.
- The 2008 Mumbai attacks, launched through the sea route, exposed glaring lapses in maritime security.
- Despite reforms, arms and narcotics landings along the Gujarat and Maharashtra coasts continue to demonstrate weaknesses.

vii. Cybersecurity and Data Sovereignty Threats

- Growing digital dependence has multiplied India's exposure to cyberattacks.
- Threats include:

- Foreign intrusions into sensitive networks.
- Ransomware attacks, such as the 2022 AIIMS breach.
- Large-scale data harvesting by external platforms, undermining privacy and sovereignty.

- Repeated intrusions into India's power grid highlight the strategic implications of such attacks.

viii. Urbanisation, Migration, and Policing Gaps

- Rapid and often unplanned urbanisation creates high-density settlements that are poorly policed.
- Migrant colonies and ghettos sometimes serve as safe houses for extremist groups.
- Communal flashpoints in urban slums illustrate how ungoverned urban spaces can quickly become security hotspots.

ix. Disasters, Climate Stress, and Health Crises as Force Multipliers

- Natural disasters and health emergencies weaken state capacity and create opportunities for hostile actors.
- Insurgents in the North-East have regrouped during flood-induced disruptions.
- The COVID-19 lockdowns coincided with spikes in smuggling and illicit cross-border trafficking.

Conclusion

India's internal security landscape is defined not only by global trends in terrorism, cybercrime, and organised crime but also by challenges that are uniquely domestic. The country's diversity, federal structure, and neighbourhood vulnerabilities make its security management both distinctive and demanding.

International models of counterterrorism and cybersecurity provide valuable lessons, but India must tailor its responses to grassroots realities—addressing alienation in border states, improving Centre–State coordination, and countering digital radicalisation.

Strengthening institutional capacities, investing in technology-enabled policing, and fostering cooperative federalism are essential for building a secure yet democratic order. As the Ministry of Home Affairs noted in 2023, more than 55% of India's internal security challenges are concentrated in less than 10% of districts, underscoring the asymmetric and localised nature of these threats.

The discussion so far has highlighted the distinct challenges that make India's internal security uniquely complex—from porous borders and ethnic diversity to technological disruptions and federal constraints. Yet, internal security cannot be fully understood in isolation. It is closely interlinked with external security, as many internal threats are fuelled or sustained by external actors. To grasp the comprehensive nature of national security, it is essential to distinguish between internal and external security, identify their overlaps, and understand how India must balance the two in an integrated framework.

1.4 Internal Security versus External Security

Internal and external security form the two central pillars of national security. While they differ in nature, scope, and institutional mechanisms, their interdependence is undeniable.

- Internal security deals with threats that emerge within the country's borders, usually from non-state actors or social fault lines, though sometimes aided by external forces.
- External security pertains to safeguarding sovereignty and territorial integrity against threats posed by foreign states and their military instruments.

In the contemporary era of hybrid warfare, cross-border terrorism, and cyber conflict, the line between internal and external security is increasingly blurred.

a. Comparative Dimensions of Internal and External Security

Aspect	Internal Security	External Security
Nature of Threat	Non-state actors (terrorists, insurgents, radical groups), occasionally backed by states	State-based military threats (enemy countries, foreign intelligence, armed forces)
Geographical Scope	Within national borders, though often linked with transnational networks	Across international borders (land, sea, air)
Primary Responsibility	Ministry of Home Affairs, Police, CAPFs, NIA, IB	Ministry of Defence, Armed Forces, Ministry of External Affairs, R&AW
Legal Instruments	UAPA, BNSS, AFSPA, PMLA, NSA	Geneva Conventions, International Humanitarian Law, Rules of War
Examples	Left-Wing Extremism, Delhi riots, cyberattacks, drone intrusions	Kargil War, Chinese incursion in Galwan, Indo-Pak War of 1971
Security Agencies	Police, CRPF, BSF, NIA, IB	Army, Navy, Air Force, Coast Guard, R&AW
Focus Area	Law & order, social harmony, counterterrorism, sabotage, organised crime	Border defence, military strategy, war preparedness
Conflict Visibility	Often covert, diffuse, or ideological	Mostly overt, visible, and strategic
Overlap Potential	High – external actors often use internal proxies	High – proxy warfare and cross-border terror blur lines

Conclusion

In today's interconnected world, internal and external threats cannot be treated in isolation. Cyber warfare, terrorism, and hybrid strategies frequently involve external adversaries operating through internal proxies, erasing the traditional distinction between battlefield and society.

India therefore requires seamless coordination between its internal and external security frameworks—integrating intelligence, technology, and institutional synergy into a unified strategy.

As Kautilya wrote in the *Arthashastra*: *"A king shall strengthen his own state and weaken the enemy's. He shall secure the welfare of his subjects by ensuring protection from both internal disorder and external aggression."* The lesson remains as relevant today: national security must be understood as a composite shield, protecting citizens against both inward and outward threats.

Safeguarding the nation is not merely a matter of force or strategy, but equally of law and governance. Internal security, in particular, must function within a constitutional democracy, where every action—whether by police, armed forces, or intelligence agencies—derives legitimacy from legal authority. Without such foundations, measures taken in the name of security risk undermining the very freedoms they are meant to protect.

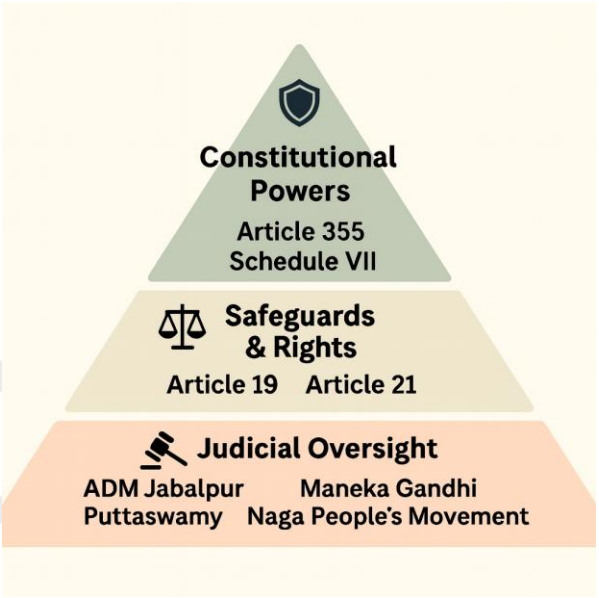
Recognising the interplay between internal and external security underscores the importance of constitutional and legal foundations. To understand how India balances liberty with protection, the

next section will examine the laws and institutional mandates that regulate the internal security apparatus.

1.5 Constitutional and Legal Framework of Internal Security

a. Introduction

India's internal security is anchored in a robust constitutional and legal framework that empowers both the Union and the states to respond to disturbances while upholding democratic norms. Although the Constitution does not explicitly use the term *"security,"* its provisions establish the basis for protecting public order, ensuring national integrity, and managing crises.



Key elements include:

- Article 355, which places a duty on the Union to protect states.
- Emergency provisions (Articles 352, 356, 360) that enable extraordinary measures in crises.
- Schedule VII, which divides powers between Union and states.
- Fundamental Rights (Articles 19 and 21), reinforced by judicial interpretation, which ensure that the pursuit of security does not undermine liberty.

This balance between authority and rights forms the constitutional backbone of India's internal security strategy.

i. Article 355: Duty of the Union to Protect States

Article 355 states: *"It shall be the duty of the Union to protect every State against external aggression and internal disturbance and to ensure that the Government of every State is carried on in accordance with the Constitution."*

- Provides constitutional justification for Union intervention in matters of internal security.
- Legal ground for deploying Central Armed Police Forces (CAPFs) or even the Army to assist states in restoring order.
- Underpins the use of Article 356 (President's Rule) and extraordinary legislations such as AFSPA.

ii. Emergency Provisions: Articles 352, 356, and 360

The Constitution empowers the Union to act in extraordinary circumstances through different forms of emergencies:

- **Article 352 – National Emergency**: Proclaimed in cases of war, external aggression, or armed rebellion. Invoked during the Punjab crisis of the 1980s on the ground of armed rebellion.
- **Article 356 – President's Rule**: Allows the Union to assume control of a state when constitutional machinery breaks down. Frequently used during periods of major internal disturbance.
- **Article 360 – Financial Emergency**: Provides for central control during financial instability. Though never invoked, it could theoretically apply in situations where unrest or disaster destabilises the economy.

iii. Schedule VII: Division of Powers

India's federal structure allocates responsibilities through the Union, State, and Concurrent Lists.

- **Union List:** Defence, armed forces, atomic energy, central agencies such as CBI and Railway Protection Force.
- **State List:** Police, public order, prisons, and forensic laboratories.
- **Concurrent List:** Criminal law, preventive detention, social justice, and related legislation.

Tension arises because while police and public order are state subjects, most serious threats—terrorism, cross-border infiltration, and organised crime—have national or transnational dimensions, requiring close Centre–State cooperation.

iv. Fundamental Rights and Internal Security

The relationship between liberty and security is most evident in the realm of Fundamental Rights:

- Article 19 – Freedoms of citizens (speech, assembly, movement) are subject to *reasonable restrictions* in the interests of sovereignty, security, and public order. These restrictions justify:
  - Internet shutdowns in Jammu and Kashmir (2019).
  - Imposition of Section 144 CrPC.
  - Curbs on public assemblies in sensitive areas.
- Article 21 – Right to life and personal liberty, expanded by judicial interpretation to include rights such as privacy (e.g., *Puttaswamy*, 2017). Article 21 acts as a safeguard against arbitrary detention and unlawful surveillance, ensuring internal security measures remain fair, just, and reasonable.

v. Judicial Contributions to the Security Framework

The judiciary has decisively shaped the contours of the security–liberty balance:

- ADM Jabalpur v. Shivkant Shukla (1976): During the Emergency, the Supreme Court controversially upheld suspension of Article 21, subordinating liberty to state power. Widely criticised.
- Maneka Gandhi v. Union of India (1978): Expanded the interpretation of personal liberty under Article 21, requiring restrictions to be *just, fair, and reasonable*.
- Justice K.S. Puttaswamy v. Union of India (2017): Recognised privacy as a fundamental right, placing significant limits on state surveillance.
- Naga People's Movement v. Union of India (1998): Placed restrictions on AFSPA's application, mandating judicial oversight of extraordinary powers.

Conclusion

The constitutional framework for internal security in India rests on a delicate balance:

- On one side lies the Union's duty to ensure order and integrity across the federation.
- On the other lies the rights and freedoms that define India as a democracy.

Constitutional provisions, emergency clauses, and federal arrangements provide the state with tools to act against threats. At the same time, fundamental rights and judicial review ensure that these powers remain accountable. Together, they form the legal scaffolding that enables India to safeguard both security and liberty—the twin pillars of a stable democratic order.

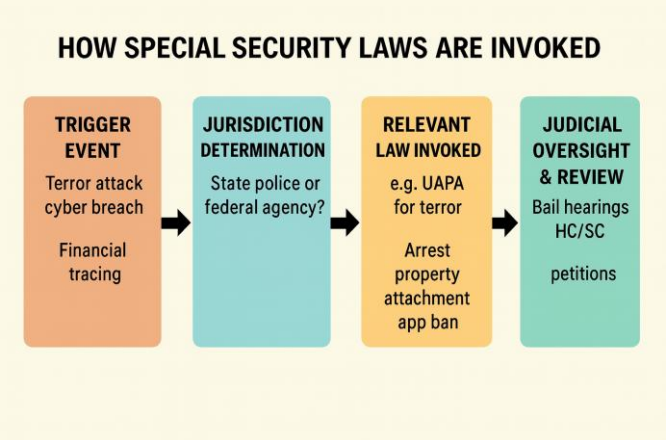
Having understood the constitutional and legal underpinnings of internal security, the next step is to explore the specific laws, institutions, and policies that operationalise this framework in practice. This will show how constitutional principles are translated into everyday governance and security measures.

1.6 Statutory and Special Security Laws

a. Introduction

India's internal security is safeguarded not only by the general criminal law framework under the Bharatiya Nyaya Sanhita (BNS) and Bharatiya Nagarik Suraksha Sanhita (BNSS), but also by a range of specialised legislations crafted to address extraordinary threats such as terrorism, insurgency, organised crime, cyber intrusions, and money laundering.

These laws aim to strike a delicate balance: enabling decisive state action against grave dangers, while remaining compatible with democratic principles and fundamental rights.



i. Unlawful Activities (Prevention) Act, 1967 (UAPA)

- Cornerstone of anti-terror architecture; initially targeted activities threatening sovereignty and integrity, later expanded after the 2008 Mumbai attacks and again in 2019 to allow individuals (not just organisations) to be designated as terrorists.
- **Key features:**
  - Declaring organisations/individuals as "terrorist."
  - Pre-charge detention up to 180 days.
  - Stringent bail provisions (Section 43D) – bail difficult unless prima facie innocence shown.
  - NIA empowered to take over investigations from state police.
- **Applications:** Bhima Koregaon case, Delhi riots 2020, Islamic State modules in Kerala.
- **Criticism:** Very low conviction rate (2.2% per NCRB, 2022); "process becomes punishment" through prolonged trials; potential political misuse.

ii. Armed Forces (Special Powers) Act, 1958 (AFSPA)

- Enacted to empower the armed forces in *"disturbed areas"* affected by insurgency and militancy.
- **Powers granted:**
  - Use of lethal force after due warning.
  - Arrest without warrant.
  - Warrantless searches.
  - Immunity from prosecution without central sanction.
- **Operational areas:** Nagaland, Manipur, parts of J&K, Arunachal Pradesh, Assam. Partial withdrawals in Nagaland and Assam reflect improving security.
- **Debates:**
  - *Jeevan Reddy Committee (2005):* Recommended repeal and merger into UAPA.
  - *Second ARC:* Suggested retention but with grievance redressal for human rights safeguards.
- **Criticism vs Support:** Critics highlight risk of rights violations; supporters argue it remains necessary in persistent insurgency zones.

iii. National Investigation Agency Act, 2008 (NIA Act)

- Created India's federal counter-terror investigative agency.
- **Key features:**
  - NIA can take over investigations from state police (departure from federal policing norm).

- 2019 amendment: Expanded jurisdiction to terror attacks on Indians abroad, human trafficking, cyber terrorism, and explosives use.

- **Notable cases:** Pathankot airbase attack, Burdwan blast, IS cases in Kerala.
- **Criticism:** States accuse NIA of eroding federalism, bypassing local police in sensitive cases.

iv. Prevention of Money Laundering Act, 2002 (PMLA)

- Enacted to combat money laundering, particularly linked to terrorism and organised crime.
- **Key provisions:**
  - Enforcement Directorate (ED) can attach tainted property, search/seize, and arrest.
  - Burden of proof shifted onto the accused.
- **Judicial validation:** *Vijay Madanlal Choudhary v. Union of India (2022)* upheld ED's powers but emphasised procedural fairness.
- **Relevance:** Closely tied to FATF compliance; often applied alongside UAPA and NDPS to tackle hawala and terror financing networks.

v. Information Technology Act, 2000 (IT Act)

- India's first comprehensive law on digital communication, cybersecurity, and e-commerce.
- **Key provisions for security:**
  - *Section 66F (Cyber Terrorism):* Criminalises attacks on critical infrastructure.
  - *Section 69A (Blocking Powers):* Govt may block websites/apps threatening sovereignty or order.
  - *Section 79 (Safe Harbour):* Immunity to intermediaries conditional on due diligence (narrowed by IT Rules 2021).
- **Recent applications:** Ban on Chinese-origin apps (e.g., TikTok) citing security; blocking disinformation portals; CERT-IN mandate for breach reporting within six hours.
- **Criticism:** Vague definitions; overbroad powers risking privacy and free speech.
- **Future:** Proposed Digital India Act, 2023 seeks to replace IT Act with a modernised framework.

vi. Other Notable Laws Relevant to Internal Security

- Maharashtra Control of Organised Crime Act, 1999 (MCOCA): State-level law to counter organised crime and underworld–terror linkages in Mumbai.
- National Security Act, 1980 (NSA): Provides for preventive detention up to 12 months to pre-empt threats to public order. Often invoked during riots or communal unrest.
- Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act): Targets drug trafficking and narco-terrorism; extensively used in Punjab to tackle drug-financed terror networks.
- Explosives Act, 1884: Regulates manufacture, transport, and use of explosives; invoked in bomb blast cases and illegal possession of explosives.

Conclusion

India's statutory and special legislations form a layered security framework. From UAPA and AFSPA to PMLA, IT Act, and NDPS, each addresses a specific dimension of threats—terrorism, insurgency, cybercrime, narcotics, or organised crime.

However, their effectiveness hinges on judicious use:

- Overreach risks eroding civil liberties and democratic trust.
- Under-enforcement weakens deterrence against dangerous actors.

The challenge lies in ensuring that these extraordinary powers are exercised in a way that strengthens both security and democratic legitimacy.

Having examined the statutory pillars of internal security, the next step is to study the institutional mechanisms and organisations tasked with implementing these laws. This will show how India's security architecture translates legal powers into operational action.

1.7 Legal Doctrines and Judicial Interpretations

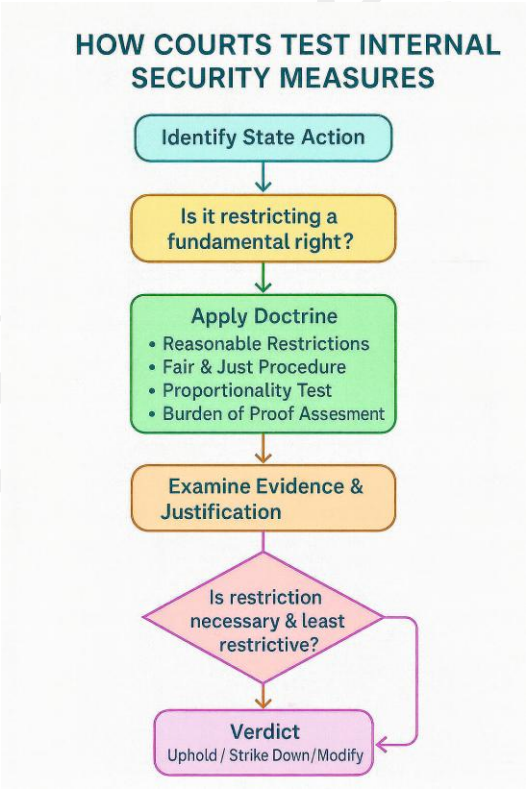
Special security legislations such as the Unlawful Activities (Prevention) Act (UAPA), the Armed Forces (Special Powers) Act (AFSPA), and the Prevention of Money Laundering Act (PMLA) confer extraordinary powers on the state. These include preventive detention, extended surveillance, seizure of assets, and restrictions on speech and assembly.

While necessary to counter grave threats, such provisions often come into tension with fundamental rights. The judiciary, as guardian of the Constitution, has therefore developed a set of legal doctrines to mediate this balance and to define the boundaries of permissible state action.

a. Key Legal Doctrines in Internal Security Jurisprudence

i. **Doctrine of Reasonable Restrictions (Article 19(2))**

- Article 19 guarantees freedoms of speech, assembly, and movement, but permits "reasonable restrictions" in the interests of sovereignty, integrity, public order, and state security.
- Justifies measures such as:
    - Internet shutdowns in Jammu & Kashmir (2019–21).
    - Banning organisations under UAPA.
    - Curbing hate speech and communal mobilisation.



ii. **Doctrine of Procedure Established by Law (Article 21)**

- India follows "procedure established by law" instead of the US-style "due process."
- *Maneka Gandhi v. Union of India (1978)* expanded its scope: procedures must be just, fair, and reasonable.
- Thus, even if a law like UAPA or NSA exists, it may be struck down if its procedures are arbitrary.

iii. **Doctrine of Proportionality**

- Requires state action restricting rights to be legitimate, necessary, least restrictive, and proportionate.
- In *Anuradha Bhasin v. Union of India (2020)*, SC ruled that internet shutdowns must be temporary, proportionate, and open to review.

iv. **Doctrine of Presumption of Innocence vs Reverse Burden**

- Normal principle: accused is innocent until proven guilty.
- Security laws like UAPA, PMLA, and NDPS reverse this presumption, placing burden on the accused (especially in bail proceedings).
- Critics argue this undermines natural justice, punishing individuals before conviction.

b. Landmark Judicial Interpretations Shaping Internal Security

i. **A.K. Gopalan v. State of Madras (1950)** – Upheld Preventive Detention Act; gave wide powers to the state. Later diluted by broader interpretations of liberty.

ii. **Maneka Gandhi v. Union of India (1978)** – Turning point; held that restrictions on liberty under Article 21 must be fair, just, and reasonable.

iii. **Justice K.S. Puttaswamy v. Union of India (2017)** – Declared privacy a fundamental right. Placed significant limits on surveillance tools (e.g., Central Monitoring System, Pegasus spyware).

iv. **Anuradha Bhasin v. Union of India (2020)** – Held that internet access is integral to free speech and business. Shutdowns under Section 144 CrPC must be temporary, proportionate, and subject to review.

v. **Naga People's Movement for Human Rights v. Union of India (1997)** – Upheld AFSPA's constitutionality but made "disturbed area" declarations subject to judicial scrutiny, imposing a limited check on extraordinary powers.

vi. **Vijay Madanlal Choudhary v. Union of India (2022)** – Upheld core provisions of PMLA, including ED's powers of arrest and attachment, but mandated recorded reasons, accountability, and judicial review to prevent abuse.

Conclusion

The judiciary's role in internal security is dual:

- It provides legitimacy to exceptional laws when necessary to protect sovereignty and order.
- It imposes constitutional limits through doctrines of fairness, proportionality, and oversight to prevent misuse.

Through landmark judgments, Indian courts have sought to ensure that the fight against terrorism, insurgency, and organised crime does not erode the democratic values these laws are meant to defend.

The discussion of constitutional provisions, statutory frameworks, and judicial doctrines illustrates the legal foundation of India's internal security. Yet laws alone cannot secure the nation—their impact depends on the institutions entrusted with enforcement. From local police stations to central armed forces and specialised intelligence agencies, India's security apparatus is vast and multi-layered. Understanding this institutional architecture is essential to grasp both its strengths and the capacity gaps adversaries seek to exploit.

1.8 Institutional and Enforcement Architecture

India's internal security is not guaranteed by laws and constitutional provisions alone. Its effectiveness depends on the institutions that enforce these frameworks on the ground. These bodies undertake tasks ranging from surveillance and intelligence gathering to counter-terror operations, cyber defence, and financial monitoring.

Operating at both central and state levels, they reflect the federal nature of Indian governance. While some agencies function exclusively under the Union government, others are autonomous at the state level. This makes coordination, clarity of roles, and accountability critical for effectiveness.

a. Central Institutions and Agencies

At the national level, the responsibility for internal security rests primarily with institutions under the Ministry of Home Affairs (MHA) and the Cabinet Secretariat. These agencies handle pan-India threats, lead policy formulation, and coordinate with state authorities.

i. Ministry of Home Affairs (MHA)

- Apex executive body for internal security.
- Controls the Central Armed Police Forces (CAPFs), the National Investigation Agency (NIA), and the Intelligence Bureau (IB).
- Oversees border management, counter-LWE policy, cyber security initiatives, and anti–terror financing measures.
- Holds authority to declare areas as *"disturbed"* under AFSPA, enabling extraordinary deployment of armed forces.

ii. Intelligence Bureau (IB)

- India's primary internal intelligence agency, operating under MHA.
- Focus areas: counterterrorism, radicalisation, Naxalism, separatist movements.
- Additional functions: political surveillance, vetting of sensitive matters such as arms licences and visas.
- Criticism: lacks statutory basis and external oversight; operates in secrecy, raising transparency concerns.

iii. National Investigation Agency (NIA)

- Established after 26/11 attacks (NIA Act, 2008).
- Jurisdiction: offences under UAPA, Explosives Act, hijacking laws, and human trafficking.
- Empowered to take over investigations across states without consent.
- *2019 amendment* expanded jurisdiction to cover crimes against Indians abroad, cyber terrorism, and explosives.
- Criticism: States allege erosion of federal policing powers; selective deployment in politically sensitive cases.

iv. National Security Council Secretariat (NSCS)

- Supports the National Security Advisor (NSA) in advising the PM on security strategy.
- Integrates intelligence from IB, R&AW, Defence Forces, cyber agencies, and diplomatic channels.
- Oversees:
    - Strategic Policy Group (SPG): senior-most coordination platform.
    - National Security Advisory Board (NSAB): expert body providing policy inputs.
    - Joint Intelligence Committee (JIC): synthesises intelligence for decision-making.
- Ensures internal security challenges are addressed in harmony with overall national security strategy.

v. Multi-Agency Centre (MAC)

- 24×7 intelligence fusion hub under the IB.
- Integrates inputs from IB, R&AW, NTRO, DIA, NIA, and state police special branches.
- State Multi-Agency Centres (SMACs) ensure decentralised reach.
- *Success:* helped pre-empt the 2011 Delhi blasts.
- Challenge: agencies often hoard intelligence, undermining timely sharing.

vi. National Intelligence Grid (NATGRID)

- Conceived after 26/11; a real-time data integration platform.
- Links 21 databases (railways, airlines, passports, banking, telecom).
- Objective: identify suspicious travel, finance, and communication patterns.
- Eleven designated agencies currently have access.
- Concerns: privacy and surveillance risks in absence of comprehensive data protection law.

vii. Enforcement Directorate (ED)

- Enforces PMLA (2002), FEMA, and Benami Transactions Act.

- Crucial in tracking terror financing and large-scale economic crimes.
- Powers: seize property, arrest suspects, and prosecute.
- Criticism: very low conviction rate (~0.5%); accused of selective targeting and political misuse.

viii. Computer Emergency Response Team – India (CERT-IN)

- Nodal body under the Ministry of Electronics and IT.
- Responds to cyber incidents: malware, ransomware, phishing, crypto scams, and website defacements.
- Issued directive mandating that cyber breaches be reported within six hours.

ix. National Critical Information Infrastructure Protection Centre (NCIIPC)

- Operates under the NTRO.
- Mandate: protect India's critical information infrastructure (power grids, telecom, banking, nuclear installations).
- Increasingly vital as state-sponsored cyberattacks target strategic assets.

x. NTRO and National Cyber Coordination Centre (NCCC)

- NTRO: Technical intelligence agency, providing signals intelligence and cyber monitoring.
- NCCC (proposed): Centralised platform to analyse internet traffic metadata for security purposes.
- Together, they strengthen India's ability to counter cyber and technical threats that blur internal–external boundaries.

India's central institutional architecture reflects both strengths and challenges: it provides layered capability, but also struggles with overlap, secrecy, and coordination issues.

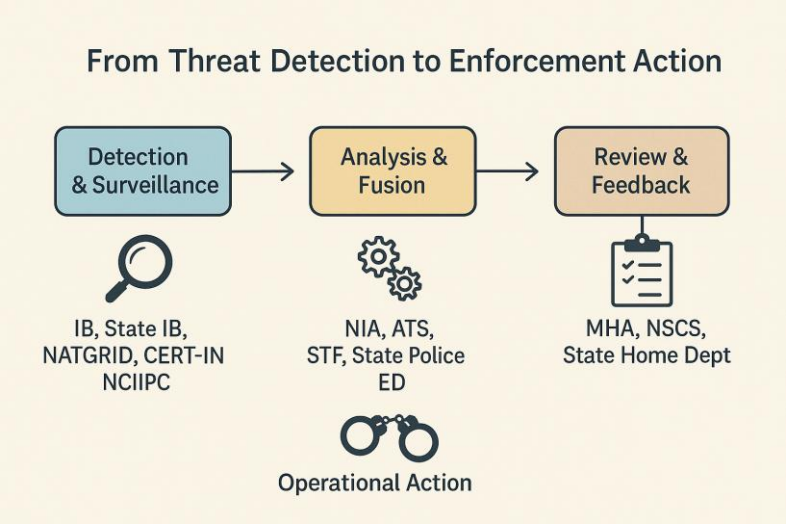
To complete the picture, it is necessary to examine the state-level security institutions—police, intelligence branches, and specialised units—that form the first line of defence against internal security threats.

b. State-Level Institutions

While central institutions provide strategic coordination and specialised capabilities, the frontline responsibility for maintaining law and order rests with the states. Under India's federal structure, *"police" and "public order"* fall under the State List of the Constitution. State-level institutions are thus the first line of defence in internal security, interfacing directly with citizens and local communities.

i. State Police Forces

- Constitutionally mandated to uphold law and order, investigate crimes, and act as first responders during riots, terrorist incidents, or communal flare-ups.
- Central to grassroots policing and immediate crisis management.
- Challenges: under-trained, under-equipped, and chronically overburdened.
- Coordination with central agencies (e.g.,



NIA, ED, MAC) is essential but often hampered by jurisdictional tensions and resource asymmetries.

ii. State Intelligence Bureaus / Special Branches

- Each state maintains an intelligence wing, often called the State Intelligence Bureau (SIB) or Special Branch.
- Focus on local-level HUMINT: monitoring radical elements, tracking community tensions, identifying triggers of violence.
- Strength: close proximity to grassroots realities.
- Weakness: capacity and effectiveness vary widely across states.

iii. Anti-Terrorism Squads (ATS)

- Established in states like Maharashtra, Gujarat, Kerala, and Uttar Pradesh.
- Specialised units tasked with:
    - Detecting and dismantling terror modules.
    - Tracking sleeper cells.
    - Monitoring online radicalisation through cyber surveillance.
- Impact: successes include foiling Islamic State recruitment networks, demonstrating the value of localised yet highly trained counter-terror forces.

iv. Special Task Forces (STFs)

- Structured as specialised operational units with legal mandates against specific threats.
- Frequently deployed to counter:
    - Narco-terrorism.
    - Arms smuggling.
    - Human trafficking.
- Their composition and tactics resemble special operations units, enabling them to conduct high-risk missions beyond the reach of conventional police.

v. State Multi-Agency Centres (SMACs)

- Function as state-level extensions of the central MAC.
- Facilitate intelligence sharing:
    - Vertically: state ↔ central agencies.
    - Horizontally: across different state institutions.
- Effectiveness: depends on timely sharing and actionable follow-up, making them vital nodes in India's intelligence grid.

Conclusion

The layered network of central and state institutions—from the MHA and intelligence agencies to state police, ATS, STFs, and SMACs—forms the backbone of India's internal security system. Together, they provide surveillance, intelligence, investigation, and operational capability across the national landscape.

Yet, the existence of institutions alone does not ensure effectiveness. Their performance is often hindered by:

- Gaps in coordination.
- Shortages of manpower.
- Technological lag.
- Overlaps of jurisdiction.

These institutional challenges explain why, despite its size and reach, India's security apparatus still struggles to prevent crises or to respond swiftly when threats materialise.

With the institutional framework now outlined, the next step is to examine the operational challenges, reforms, and capacity-building measures necessary to make India's internal security architecture more agile, accountable, and technologically equipped.

1.9 Institutional Challenges in India's Internal Security Architecture

a. Introduction

India has created a vast institutional framework for internal security, combining central and state agencies across intelligence, policing, financial enforcement, and cyber defence. Yet the effectiveness of this apparatus is often undermined by institutional inefficiencies. Overlapping jurisdictions, fragmented intelligence flows, Centre–State friction, weak statutory bases, technological lag, and human resource shortages repeatedly erode the system's capacity for timely and coordinated response.

i. Overlapping Jurisdictions

- Multiple agencies frequently investigate the same or related cases.
- IB, NIA, ED, state police, and Anti-Terrorism Squads often duplicate efforts, leading to turf wars and wasted resources.
- Example: Parallel investigations by the NIA and state police under UAPA have produced friction instead of synergy.

ii. Fragmented Intelligence Sharing

- Despite the creation of MAC and SMACs, intelligence sharing remains fragmented and delayed.
- A "need-to-know" rather than "need-to-share" culture persists.
- Bureaucratic hierarchies cause critical inputs to be hoarded or diluted, creating gaps between collection and actionable field intelligence.

iii. Centre–State Friction

- Federal division of powers complicates coordination.
- Since *law and order* is a state subject, states often see central agencies like NIA or ED as encroachments on autonomy.
- Recent tensions between states such as West Bengal and Maharashtra and central bodies illustrate how politics obstructs operational efficiency.

iv. Lack of Statutory Backing

- Key agencies—including the IB, MAC, and NSCS—operate without explicit legislative sanction, relying on executive orders.
- This weakens accountability and limits their resilience against judicial scrutiny.
- By contrast, NIA and ED enjoy stronger legitimacy through statutory foundations.

v. Technological Deficiencies

- Security threats are increasingly digital, but most agencies—especially at the state level—remain technologically underprepared.

- Advanced capabilities like cyber forensics, AI-enabled surveillance, big data analytics, and OSINT remain confined to elite institutions such as CERT-IN and NTRO.
- The uneven distribution of technology leaves vast regions exposed and vulnerable.

vi. Human Resource Gaps

- Police-to-population ratio: 156 per lakh, well below the UN norm of 222.
- Vacancies in police and intelligence units often exceed 25%.
- Acute shortage of specialists: cyber investigators, linguists, forensic experts, and digital analysts.
- In an era of hybrid and tech-driven threats, these deficits leave frontline institutions ill-prepared.

Conclusion

The institutional challenges facing India's internal security cannot be solved through piecemeal fixes. They demand systemic reform:

- Clear mandates to eliminate overlaps.
- Institutionalised mechanisms for seamless, real-time intelligence sharing.
- Statutory legitimacy for core agencies like IB and MAC to ensure accountability.
- Sustained investment in cutting-edge technology e.g., AI, big data, predictive surveillance.
- Expanded manpower with specialised training in cyber, forensic, and linguistic domains.

As highlighted in global security discourse: *"Security is not the absence of threat, but the presence of strong institutions that can respond to it swiftly and justly."* This principle is as relevant to India today as to any democracy seeking to balance liberty with resilience.

The discussion so far has explored the conceptual foundations of internal security in India: its scope, challenges, legal framework, and institutional enforcement. Yet security is not merely about force, laws, or intelligence coordination. It is deeply tied to social and economic development.

Persistent underdevelopment, inequality, and exclusion often create fertile ground for unrest, radicalisation, and conflict. Insurgency in the North-East, Left-Wing Extremism in central India, and communal volatility in urban centres all point to the same truth: development and security are inseparably linked.

To grasp internal security in its full dimension, the next chapter turns to the development–security nexus—how the absence of development fuels insecurity, and how insecurity obstructs development.

Chapter 2. Development–Security Nexus

2.1 Extremism: Meaning and Significance

Extremism may be understood as the holding of radical views or ideologies that sharply deviate from a society's broadly accepted norms and constitutional values. It is marked by intolerance, rigidity, and, in many cases, a willingness to justify authoritarianism or violence.

In India, extremism becomes a national security challenge when it:

- Translates into violent movements or ideologically driven insurgencies.
- Undermines democratic institutions and constitutional governance.
- Erodes the fragile fabric of social harmony and cohesion.

As has been noted: *"Extremism is not just about what is thought — but what is justified, what is advocated, and what is done in its name."*

a. Core Features of the Extremist Mindset

The psychology of extremism is shaped by recurring patterns of thought and behaviour:

- **Ideological Rigidity** – Unshakeable belief in the superiority of one's worldview, rejection of compromise or dialogue.
- **Moral Absolutism** – A conviction that one's position is unquestionably right, rendering all others illegitimate.
- **Us versus Them Narrative** – Creation of binaries such as *pure vs corrupt* or *oppressed vs oppressor*, encouraging hostility.
- **Rejection of Pluralism** – Intolerance of religious, caste, linguistic, or socio-economic diversity.
- **Willingness to Use Violence** – Acceptance or advocacy of violence as a legitimate means to achieve goals.

Not all extremists are violent, but most violent actors—terrorists, insurgents, or radical groups—draw sustenance from extremist ideologies.

b. Classification of Extremism in India

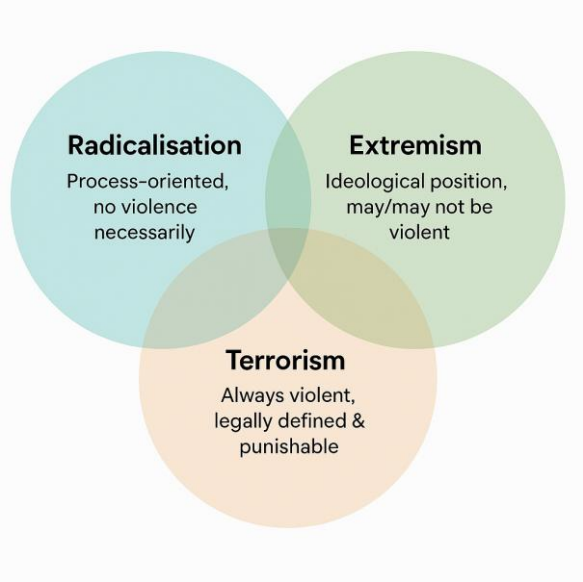
Extremism manifests in multiple forms, reflecting India's diverse social, political, and regional context:

- **Left-Wing Extremism (LWE):** Represented by Maoists/Naxalites, advocating armed revolution and redistribution of resources.
- **Right-Wing Extremism:** Ultra-nationalist or communal groups (e.g., vigilante networks) that thrive on polarisation and mob violence.
- **Religious Extremism:** Islamist radical outfits as well as fringe Hindutva groups using theological justification for violence.
- **Ethnic and Regional Extremism:** Secessionist groups like ULFA, NSCN (IM), or Khalistani revivalist networks mobilising identity-based grievances.
- **Issue-Based Extremism:** Radical groups opposing dams, mining, or infrastructure projects; sometimes resorting to sabotage or violent protest.
- **Digital Extremism:** Fast-growing form using platforms like Telegram, YouTube, Instagram for radicalisation, recruitment, and transnational propaganda.

c. Extremism, Radicalisation, and Terrorism: Distinguishing the Concepts

Although often used interchangeably, these represent different stages of the threat spectrum:

- **Radicalisation** – The process of adopting extreme views; not inherently violent and not a crime under Indian law.
- **Extremism** – Holding/spreading intolerant ideologies that oppose constitutional values; may or may not involve violence, and its legal status is ambiguous.
- **Terrorism** – The use of violence to instil fear and achieve political or ideological ends; explicitly defined and punishable under statutes such as UAPA.



Conclusion

The discussion clarifies the meaning, mindset, and forms of extremism, as well as its linkages with radicalisation and terrorism. Importantly, extremism is not static—it evolves with social, political, and technological shifts.

India's post-independence history reveals that extremism has taken different shapes at different times:

- Early secessionist movements in border states.
- Ideological insurgencies like Naxalism and Khalistani militancy.
- Contemporary digital radicalisation spread via global networks.

This trajectory shows that extremism often mirrors the developmental and political tensions of the period. To understand this dynamic fully, it is necessary to trace the evolution of extremism in India after 1947—a task taken up in the next section.

2.2 Evolution of Extremism in India after 1947

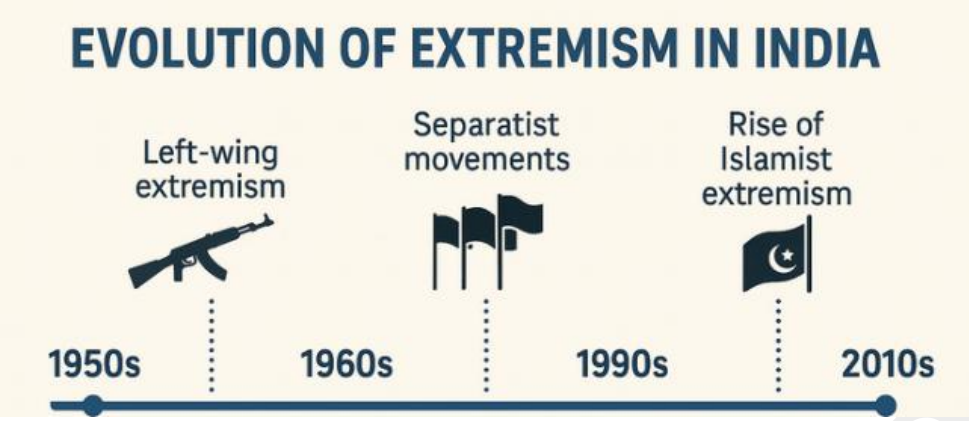
Since Independence, India's internal security has been reshaped repeatedly by waves of extremism. These movements—rooted in ethnic identity, ideology, socio-economic grievances, or religion—share a common feature: challenging the authority of the state and undermining national cohesion.

Unlike conventional threats, extremism in India is adaptive: it draws sustenance from local grievances while at times aligning with global ideological currents or receiving external support. From ethno-regional insurgencies in the Northeast, to Maoist class struggles, to militancy in Punjab and Kashmir, and more recently to digital radicalisation, the trajectory of extremism reflects India's shifting developmental and political tensions.

a. Concise Historical Overview

i. **1950s–1960s: Ethnic Insurgencies in the Northeast**

- The first major internal security challenge after Independence.
- The Naga National Council (NNC) launched an armed insurgency in 1956 against forced integration into India.
- The Indian Army was deployed in the Naga Hills; insurgency later spread to Mizoram and other parts of the Northeast.



ii. **1967 onwards: Left-Wing Extremism (LWE)**

- The Naxalbari uprising in West Bengal, led by Charu Majumdar and Kanu Sanyal, called for armed revolution against the state.
- Inspired by Maoism, it spread to rural and tribal belts, becoming a nationwide ideological challenge.

iii. **1980s: Khalistani Extremism in Punjab**

- Religious separatism surfaced, with groups such as Babbar Khalsa and the Khalistan Commando Force demanding an independent Sikh state.
- Events like Operation Blue Star (1984) and the anti-Sikh riots intensified militancy, leading to a decade-long insurgency.

iv. **1990s: Islamist Terrorism and Cross-Border Infiltration**

- The insurgency in Jammu & Kashmir escalated, heavily supported by Pakistan's ISI.
- Groups such as Lashkar-e-Taiba and Hizbul Mujahideen, along with domestic outfits like SIMI and later the Indian Mujahideen, entrenched religious extremism as a national concern.

v. **2000s–2010s: Urban Extremism and "Urban Naxals"**

- Beyond rural insurgency, ideological networks grew in urban spaces.
- Intellectuals, NGOs, and activists were alleged to provide support, as seen in the Bhima Koregaon case (2018).
- Highlighted the state's concern with non-combat logistical and ideological support networks.

vi. **Present Day: Hybrid and Multi-Dimensional Extremism**

- Contemporary extremism blends multiple strands:
  - Residual Maoist insurgency.
  - Ethnic militancy in parts of the Northeast.
  - Islamist modules with cross-border linkages.
  - Digital radicalisation via YouTube, Telegram, Instagram—making extremism borderless and decentralised.

b. Timeline of Left-Wing Extremism (1967–Present)

i. **1967–1970s: Origins and Consolidation**

- Triggered by Naxalbari uprising (1967).
- Formation of CPI (Marxist–Leninist) in 1969 provided ideological coherence.

ii. **1980s–1990s: Expansion**

- People's War Group (PWG) emerged in 1980, spreading operations to Andhra Pradesh and Odisha.

- By the 1990s, violence extended to Bihar and Jharkhand.
- Brutal massacres such as Bara (1992) and Senari (1999) marked the period.

iii. **2000s: Peak Insurgency and State Response**

- 2004 merger: PWG + Maoist Communist Centre → CPI (Maoist).
- Expanded across the "Red Corridor."
- Characterised by high-casualty ambushes, prison breaks, and widespread use of IEDs.
- State response included:
    - Greyhounds (Andhra Pradesh) for counter-insurgency.
    - Integrated Action Plan (IAP) for development in affected districts.

iv. **2010s: Decline and Tactical Shifts**

- Deaths of leaders like Kishenji (2011) weakened the movement.
- Violence contracted geographically, though major ambushes continued (e.g., Sukma 2017, Gadchiroli 2019).
- Greater reliance on urban ideological networks.

v. **2020s–Present: Containment and Endgame**

- By early 2020s, LWE violence had sharply declined.
- Operations like Operation Kagar confined Maoists to small forested pockets in Chhattisgarh, Jharkhand, Odisha.
- Neutralisation of leaders such as Nambala Keshava Rao has weakened the movement.
- Government targets elimination of LWE by 2026.

c. Shifts in the Nature of Grievances

The sources of extremism in India have shifted with changing socio-economic and political realities:

- **1950s–1970s:** Ethnic identity, autonomy, and land rights (e.g., Naga and Mizo insurgencies).
- **1970s–1990s:** Class conflict and agrarian inequality (e.g., Naxalbari uprising, Maoist movements).
- **1980s–1990s:** Religious separatism (e.g., Khalistan militancy, Kashmir insurgency).
- **2000s–2020s:** Alienation combined with digital radicalisation (e.g., urban Maoism, ISIS recruitment online).

This trajectory underscores that internal security threats are not uniform but adaptive, evolving in response to new grievances and external influences. From secessionist movements and class struggles to religious radicalisation and cyber extremism, each wave has posed unique threats to India's stability. Security strategies, therefore, must be equally dynamic, integrating law enforcement with political dialogue, socio-economic reforms, and technological preparedness.

d. Transformation in Operational Style

Extremism in India has undergone profound changes in its methods of recruitment, organisation, and communication:

- **Recruitment:** Earlier, mobilisation occurred through village-level cells and personal persuasion. Today, indoctrination happens largely online, via encrypted apps and social media.
- **Structure:** Guerrilla forest camps have been supplemented—or replaced—by dispersed sleeper cells and lone-wolf actors. Decentralised networks are harder to detect.
- **Support Base:** While rural tribals and peasants formed the original base, contemporary extremism often draws on urban intellectual circles, NGOs, and diaspora funding channels.

- **Communication:** Word-of-mouth and pamphlets have given way to WhatsApp groups, Telegram channels, and dark web forums, enabling secrecy and cross-border reach.

This shift illustrates how extremism adapts to new technologies and urban contexts, making it more insidious and less visible to traditional counterinsurgency strategies.

e. Rise of Cross-Border and Global Linkages

India's extremism has rarely been an entirely domestic phenomenon—it has often been enabled or amplified by external actors:

- Pakistan's ISI has supported Khalistani groups in Punjab and militant outfits in Jammu & Kashmir.
- Insurgents in the Northeast have used safe havens in Myanmar and received occasional support from China.
- Gulf-based organisations have provided funding and ideological backing to radical elements.
- In recent years, global jihadist narratives from the Islamic State have inspired modules in Kerala, Telangana, and beyond, linking local radicalisation to transnational currents.

These developments confirm that extremism in India is inseparable from global security trends, requiring both internal resilience and international cooperation.

f. Evolving State Response

The Indian state's approach to extremism has transformed significantly across decades:

- **1950s–1980s:** Heavy reliance on military suppression, use of AFSPA, and large-scale counterinsurgency operations.
- **1990s–2000s:** Creation of specialised forces (e.g., Greyhounds in Andhra Pradesh, CoBRA for anti-Maoist ops) alongside surrender and rehabilitation policies.
- **Post-2010:** Shift to an integrated approach combining security with development initiatives (e.g., SAMADHAN doctrine, Aspirational Districts programme) and greater reliance on digital surveillance.
- **Present Day:** Focus on "smart" technologies, counter-radicalisation, and community engagement, aiming to address both manifestations and root causes of extremism.

Conclusion

The evolution of extremism in India reflects a journey from region-specific insurgencies to hybrid, technology-enabled threats with global linkages. While actors and methods have changed, the underlying drivers—alienation, inequality, and external interference—remain persistent.

Thus, the state's response must be equally adaptive: combining development, decentralised governance, and tech-enabled policing with ideological counter-narratives that restore faith in democracy.

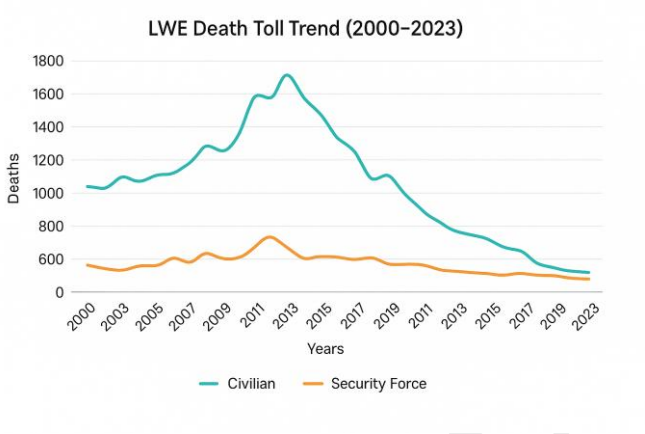
As Dr. Manmohan Singh aptly observed on Left-Wing Extremism:
"You cannot fight extremism with bullets alone. You need to fight it with education, inclusion, and hope."

India has witnessed many extremist movements flare and recede—ethnic insurgencies in the Northeast, Khalistani separatism in Punjab, and Islamist militancy in Kashmir. Yet one movement has shown extraordinary persistence: Left-Wing Extremism (LWE). Born in the late 1960s out of agrarian inequality, it expanded into a sprawling insurgency across the "Red Corridor," once described by the Prime Minister as the single biggest internal security challenge.

To understand why this movement endured for decades, and how it reshaped governance, society, and development, the next section examines the impact of Left-Wing Extremism in detail.

2.3 Impact of Left-Wing Extremism (LWE)

a. Introduction



Left-Wing Extremism (LWE), often referred to as the Naxalite–Maoist insurgency, has been one of India's longest-running and most complex internal security challenges.

- As per the Ministry of Home Affairs' Security Related Expenditure (SRE) Scheme, the number of affected districts has declined from 223 in 2008 to 45 in 2023 to 22 in 2025.
- Yet, violence remains concentrated in core strongholds such as Sukma (Chhattisgarh), Gadchiroli (Maharashtra), and Malkangiri (Odisha).

The LWE threat is multidimensional:

- It erodes state authority in remote tribal belts.
- It perpetuates a *"conflict trap"* where violence blocks development and underdevelopment fuels violence.
- It combines Maoist ideology with local grievances like land alienation, mining-related displacement, and denial of forest rights.

i. Socio-Economic Impact

Disruption of Essential Services

- Education severely affected: schools shut during Maoist "bandhs" or destroyed to prevent use as security camps.
- In Bastar, over 200 schools were demolished (2006–2010).
- Health services curtailed: attacks on sub-centres and threats to health staff hinder maternal care, immunisation, and epidemic response.
- Targeting of bridges and telecom towers isolates villages, delaying emergency relief.

Fear Among Government Staff

- Teachers, health workers, and block officers operate under threats of abduction or assassination.
- Example: In 2009, a block development officer in Jharkhand was killed for refusing to divert PDS grain to Maoist cadres.

Development Deficits

- Contractors withdraw from projects due to Maoist extortion (~10–30% of costs).
- Chronic under-spending of flagship schemes such as PMGSY and NRLM deepens alienation and reinforces underdevelopment.

ii. Human Security Impact

Loss of Life

- Since 2000, over 12,000 deaths from LWE-related violence.
- In many years, civilian deaths outnumber those of security personnel.

Mass Displacement

- Counter-insurgency operations and reprisals uproot thousands.

- *Salwa Judum* (2005–2011) displaced over 50,000 tribals in Chhattisgarh.

Suppression of Democratic Rights

- Maoists enforce election boycotts, threatening villagers.
- In the 2019 Lok Sabha polls, Dantewada saw only 25% turnout, far below the national average.

Psychological Impact

- Long exposure to violence creates a climate of fear, especially among youth.
- Propaganda portraying the state as corrupt erodes trust in governance and fosters insurgent sympathy.

iii. Economic Impact

Targeting Critical Infrastructure

- Attacks on railways, bridges, and mining convoys disrupt economies.
- Example: repeated sabotage of the Kirandul–Kothavalasa railway line crippled iron ore transport in Chhattisgarh.
- Power transmission lines are frequently hit, causing prolonged blackouts.

Extortion and "Revolutionary Tax"

- Levies on mining companies, contractors, and traders inflate project costs.
- Such coercion discourages investment and drains local economies.

Deterrence to Private Investment

- Despite being resource-rich, LWE districts remain unattractive to investors.
- Iron ore extraction in Dantewada, for instance, remains well below potential.

iv. Political Impact

Parallel Governance

- Maoists conduct "Jan Adalats" delivering swift but brutal punishments.
- This bypasses and delegitimises grassroots institutions like panchayati raj bodies.

Election Sabotage

- Polling booths destroyed, EVMs burnt, candidates attacked.
- Distorts democratic representation and weakens legitimacy of elected governments.

Erosion of State Legitimacy

- Inability to guarantee security in its own territory emboldens insurgents.
- Creates "stateless zones" where governance is effectively replaced by Maoist authority.

Conclusion

The impact of LWE extends far beyond armed encounters. It corrodes governance, fragments communities, weakens democracy, and stifles development in some of India's most resource-rich yet under-served regions.

Security operations are vital to reclaim control, but they cannot secure durable peace alone. Resolution requires addressing structural grievances—land rights, tribal representation, and fair resource-sharing. Only by blending:

- Security operations,
- Inclusive development, and
- Rights-based governance,

can India break the cycle of alienation and violence.

As Dr. Manmohan Singh observed:
"You cannot fight extremism with bullets alone. You need to fight it with education, inclusion, and hope."

The case of LWE demonstrates how unresolved grievances plus weak governance can fuel decades of conflict and block development. Yet LWE is only one strand in India's evolving security landscape.

The past decade has witnessed the rise of new-age threats—cross-border terrorism, cyber intrusions, radicalisation through social media, drone smuggling, and hybrid warfare. To design a comprehensive strategy, it is essential to move beyond single case studies and assess the emerging trends and concerns in India's internal security as a whole.

2.4 Current Trends and Concerns in Internal Security

a. Introduction

India's internal security paradigm is undergoing profound transformation. While earlier decades were dominated by insurgencies in jungles or separatist struggles in border states, contemporary threats are increasingly diffuse, networked, and technology-driven. Extremism today no longer confines itself to remote geographies; it unfolds in encrypted chats, digital platforms, academic debates, and even courtrooms.

New-age threats are marked by blurred boundaries—between ideology and organised crime, between dissent and subversion, and between state and non-state actors. Hybrid extremism, deepfake propaganda, cryptocurrency financing, and intellectual front organisations have shifted the battlefront from the physical to the psychological, from the visible to the virtual. Detecting and dismantling such challenges is far more complex than conventional policing.

i. Hybrid Extremism

- Hybrid extremism blends multiple socio-political grievances—caste, religion, class, or regional identity—into a single mobilisation framework.
- Groups increasingly invoke intersectional narratives: e.g., combining Dalit victimhood, religious injustice, and anti-establishment rhetoric.
- Such adaptability makes movements harder to categorise and resistant to conventional counter-narratives, since they appeal across diverse constituencies simultaneously.

ii. Deepfake and AI-Powered Radical Content

- The accessibility of artificial intelligence tools has empowered extremist actors to fabricate convincing videos, voices, and messages.
- Examples include:
    - Communal incitement videos,
    - Fake clips impersonating security officials,
    - Disinformation designed to provoke riots.

- In 2023, Punjab Police flagged deepfake videos impersonating police personnel to circulate pro-Khalistan propaganda.
- The key challenge: speed of spread on encrypted platforms far outpaces fact-checking or official counter-statements.

iii. Cryptocurrency and Dark Web Financing

- Extremist networks increasingly use digital currencies (Bitcoin, Monero, etc.) for anonymous transfers.
- Uses include:
    - Receiving funds from foreign sympathisers,
    - Purchasing weapons and forged documents on dark web marketplaces,
    - Paying local operatives.
- Example: A Tamil Nadu IS module received crypto payments for recruitment.
- Weakness: Indian law enforcement still lacks robust capacity to trace blockchain trails or decrypt wallets, leaving investigative blind spots.

iv. Crime–Terror Overlap

- The convergence of organised crime and extremism has deepened.
- Drug cartels, arms smugglers, and human traffickers increasingly enable extremist violence.
- Example: Intelligence reports suggest Golden Triangle drug cartels channelled funds to Maoist cadres in exchange for jungle smuggling routes.
- This transforms terrorism from an ideological project into a self-financing criminal enterprise.

v. Urban Maoism

- Refers to the intellectual and logistical ecosystem supporting violent Maoist movements.
- Operates via universities, NGOs, media outlets, and legal activism.
- Urban actors function as "invisible generals," guiding cadres through encrypted communication or strategy papers.
- Example: The Bhima Koregaon case (2018) revealed discussions of "Rajiv Gandhi–like" attacks and alleged urban networks funding field operatives.
- Unlike forest guerrillas, these actors are educated, media-savvy, and embedded in democratic institutions, making state response politically sensitive and legally complex.

vi. State and Non-State Actors: Blurred Boundaries

- Extremism in India often arises from non-state groups, but many enjoy external state patronage or safe havens.
- Examples:
    - Non-state: CPI (Maoist), SIMI, Indian Mujahideen, ULFA, ISIS-inspired cells.
    - State-sponsored: Pakistan's ISI funds and trains Kashmiri and Khalistani modules.
    - Hybrid actors: Urban Maoists legitimise violence while avoiding direct culpability.
- This reflects asymmetric warfare, where adversarial states exploit internal vulnerabilities through proxies and ideology.

Conclusion

India's internal security environment is now shaped by decentralised, hybrid, and tech-enabled threats. From jungle insurgents to digital radicals, from narco-terrorism to deepfake propaganda, the spectrum is both vast and evolving. Combating these requires a paradigm shift:

- From force-based policing to intelligence-led, tech-driven disruption,
- From reactive responses to proactive ecosystem targeting,
- From muscle to mind, uniform to algorithm.

As one analyst observed:
"From the jungle to the courtroom to the algorithm, modern extremism wears many masks. India's internal security must adapt from muscle to mind, from uniform to algorithm."

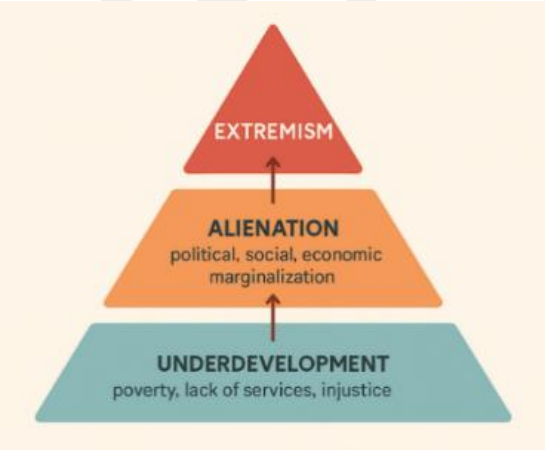
The survey of these trends highlights a paradox: while methods have become digital and hybrid, the roots of extremism remain social and developmental. Alienation, poverty, displacement, and denial of dignity continue to supply oxygen to extremist mobilisation.

This leads us directly to the development–security nexus, which explains why some regions remain vulnerable to extremism while others stay resilient. The next section will explore how underdevelopment and alienation interact with extremism in shaping India's internal security landscape.

2.5 Underdevelopment, Alienation and Extremism

a. Introduction

Internal security in India cannot be disentangled from its development trajectory. In conflict-prone regions—whether along the Maoist-affected "Red Corridor," the insurgency-ridden Northeast, or marginalised urban settlements—decades of underdevelopment and systemic neglect have created fertile ground for alienation and extremist mobilisation.



When citizens lack access to basic services, equitable representation, and trust in institutions, grievances are not merely expressed but weaponised. Resistance born of deprivation often hardens into extremism, creating a vicious cycle: weak governance invites parallel authority, insurgency cripples developmental efforts, and continued underdevelopment fuels further alienation.

Breaking this cycle requires the state to be more than an enforcer of law—it must become a visible and empathetic provider of justice, dignity, and opportunity.

b. Key Concepts

- **Underdevelopment:** Persistent poverty and the absence of basic services such as roads, schools, healthcare, and jobs.
- **Alienation:** The perception or reality of political, social, and economic marginalisation from the national mainstream.
- **Extremism:** The adoption of violent or radical means to resist perceived injustice, often targeting the state as illegitimate.

c. How Underdevelopment Fuels Insecurity

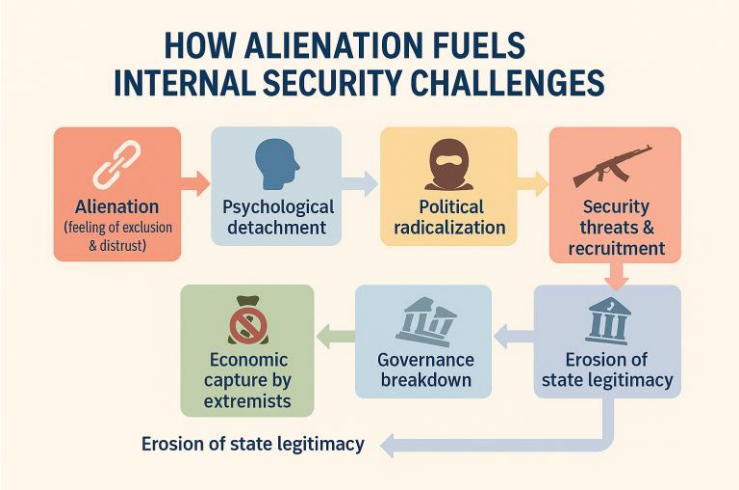
i. State Absence and Parallel Authority

- In many LWE strongholds and remote border areas, the state is visibly absent.
- Lack of schools, banks, ration shops, and roads leaves citizens with little experience of welfare governance.
- Extremist groups step into this vacuum by running "Jan Adalats" (people's courts), providing rudimentary healthcare, or offering protection.

- In Bastar, Maoist "courts" often resolve land disputes more swiftly than state institutions, reinforcing their legitimacy.

ii. Economic Exploitation without Compensation

- Industrial projects (mining, dams, SEZs) often displace local communities without proper rehabilitation.
- Environmental degradation and alienation from *jal–jungle–zameen* (water–forest–land) deepen resentment.
- Communities view the state as a facilitator of private capital rather than a defender of tribal rights.
- Protests against projects by POSCO and Vedanta in Odisha and Chhattisgarh illustrate this dynamic.



iii. Poverty as a Recruitment Pool

- In jobless, underdeveloped districts, youth see few prospects.
- Maoist groups lure them with small stipends, rations, and dignity through armed struggle.
- MHA estimates suggest most Maoist foot soldiers are 16–25 years old with minimal education.

iv. Loss of Trust in Democratic Institutions

- Delayed trials, fake encounters, and custodial torture foster mistrust.
- Citizens often view the state as a source of injustice rather than protection.
- Alleged encounter killings in Dantewada and Bijapur have been used in Maoist propaganda for recruitment.

v. Communication and Perception Gaps

- Mainstream media rarely penetrates insurgency zones.
- Poor representation of tribal languages and concerns widens alienation.
- Extremists monopolise narratives through identity-based propaganda.
- Lack of grievance redress in local languages—via apps, radio, or field officials—further disconnects citizens from the state.

vi. Security–Development Disconnect

- Development projects often ignore ground security conditions.
- Roads built without adequate security are quickly destroyed.
- Contractors withdraw under Maoist extortion, leaving incomplete projects and wasted funds.
- Maoists sabotage mobile towers, Anganwadi centres, and schools, ensuring the development vacuum persists.

vii. Regional Illustrations

- Bastar (Chhattisgarh): Tribal land alienation and allegations of security force excesses sustain Maoist mobilisation.
- Dantewada (Chhattisgarh): Poor connectivity and weak banking create dependence on Maoist taxation.
- Jungle Mahal (West Bengal): Long socio-economic neglect enabled Maoist dominance (2009–2011) until state recovery operations reclaimed the area.

Conclusion

Extremism thrives where the state is absent, justice is delayed, and development is denied. Breaking this cycle requires security to be integrated with inclusive governance and visible development. The most effective counter to insurgency is not coercion alone, but a state that delivers dignity, fairness, and opportunity.

As one analyst observed: *"The absence of governance is not neutrality — it is a vacuum that gets filled by coercive non-state actors."*

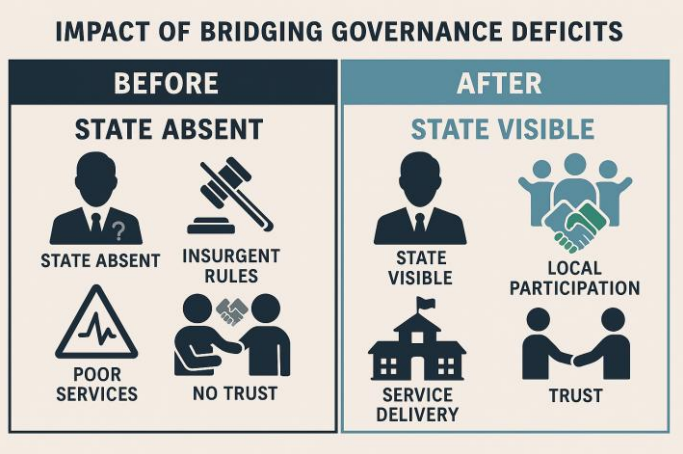
The link between underdevelopment, alienation, and extremism demonstrates that violence does not emerge in a vacuum—it grows where governance is weak or unresponsive. This raises a deeper structural question: why do some districts remain persistently vulnerable to conflict while others, equally poor, remain relatively stable? The answer lies in the governance deficits of conflict-prone areas, where state institutions struggle to project authority, build trust, and sustain development in the face of difficult geography, weak capacity, and entrenched inequalities.

The next section will therefore turn to these governance deficits to explain why certain regions remain perpetual hotspots of extremism.

2.6 Governance Deficits in Conflict-Prone and Remote Areas

a. Introduction

Governance deficit refers to the failure or absence of the state's institutional presence, responsiveness, and service delivery in violence-prone, tribal, border, or insurgency-affected regions. In India, such deficits are most acute in the Maoist-affected Red Corridor, the insurgency-prone Northeast, parts of Jammu and Kashmir, and sensitive border districts.



These gaps weaken the legitimacy of the state, allow insurgents to assume roles as parallel power centres, and foster a cycle of alienation, grievance, and radicalisation. Understanding the specific dimensions and causes of governance deficits is essential to designing credible responses.

b. Key Characteristics of Governance Deficit

- **Administrative:** Sparse or absent presence of civil authorities such as District Magistrates, Block Development Officers, or Tehsildars in remote areas.
- **Developmental:** Poor infrastructure and inadequate access to basic services such as roads, electricity, schools, hospitals, and telecom.
- **Security:** Limited police presence, inadequate surveillance, and delayed response to incidents.
- **Judicial:** Non-functional or understaffed courts, lack of legal aid, and slow justice delivery.
- **Financial:** Leakages in welfare schemes and prevalence of "banking deserts" with little access to formal financial institutions.
- **Political:** Weak Panchayati Raj institutions and inadequate representation of tribal or marginalised communities in governance.

c. Real-World Illustrations

- **Dantewada and Sukma (Chhattisgarh):** Vacant health centres, absence of banking, and poor road access allow Maoists to run parallel justice systems and tax economies.
- **Arunachal Pradesh interiors:** Villages often lie over 100 kilometres from the nearest administrative office, enabling insurgent groups to command loyalty.
- **Manipur hills:** Weak schooling and poor electricity supply create space for ethnic militias to provide parallel governance.
- **Border villages in Jammu and Kashmir:** Lack of internet access and delays in welfare delivery foster disaffection and cross-border infiltration.

d. Core Problems Feeding the Governance Deficit

- **Fear of Violence and Risks to Officials**
  - Civil servants, teachers, doctors, and engineers frequently refuse postings or exit prematurely due to threats of ambush, kidnapping, or assassination.
  - Even family members are targeted. In Sukma, the District Collector's office itself was once attacked.
  - Governance becomes "postal"—schemes exist on paper but lack execution.
- **Inaccessible Terrain and Infrastructural Backwardness**
  - Conflict-prone areas are often hilly, forested, or riverine, with poor connectivity.
  - In Gadchiroli or Upper Subansiri, reaching a panchayat HQ can take 6–10 hours.
  - Disasters like floods and landslides worsen isolation.
- **Deliberate Sabotage by Insurgents**
  - Extremists target development projects to maintain their relevance.
  - Bridges blown up, schools burnt, contractors threatened—Jharkhand and Chhattisgarh have seen dozens of such cases.
- **Corruption, Leakages, and Weak Accountability**
  - Welfare funds diverted via ghost records and middlemen.
  - Weak auditing, little media presence, and minimal civil society oversight foster corruption.
  - For citizens, the state becomes associated with extraction, not empowerment.
- **Manpower Shortages and Vacancies**
  - Chronic understaffing in BDOs, schools, and PHCs.
  - Staff often come from outside, lacking cultural familiarity, and many leave early due to poor conditions and insecurity.
- **Digital and Financial Exclusion**
  - Aadhaar-linked DBT systems collapse in areas without internet.
  - Banking deserts force villagers to travel 30–60 km for pensions or MGNREGA wages.
  - Lack of Common Service Centres or grievance platforms widens exclusion.
- **Cultural Disconnect and Insensitive Bureaucracy**
  - Officials unfamiliar with tribal customs, dialects, and priorities alienate communities.
  - Top-down schemes imposed without consultation fuel resentment and fears of cultural erosion.

Conclusion

Governance deficits in conflict-affected areas corrode state legitimacy and enable insurgents to act as alternative authorities. When the state fails to deliver security, services, and justice, coercive parallel systems quickly fill the void. Closing this gap requires more than infrastructure—it demands

culturally sensitive administration, visible and accountable institutions, and sustained trust-building with local communities.

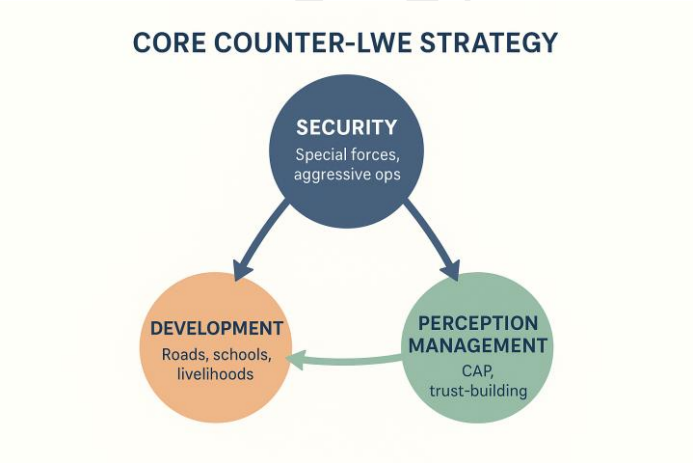
As K.P.S. Gill observed: *"When the State does not arrive, the insurgent becomes the administrator. And when it arrives too late, it becomes the enemy."*

The persistence of governance deficits shows that insurgency endures not merely on ideology or external support but on the daily vacuum in service delivery and state presence. Recognising this, successive governments have attempted to bridge these gaps through targeted policies, special schemes, and administrative innovations.

The next section therefore examines these state interventions, assessing their design, implementation, and effectiveness in reducing alienation and restoring legitimacy.

2.7 Addressing Governance Deficits in Conflict-Prone Areas: The Indian Experience

a. Introduction



India's governance strategy in conflict-affected regions has steadily evolved from a force-centric model to one that blends security, development, and trust-building. Recognising that coercion alone cannot resolve deep-rooted grievances, the state has adopted multi-dimensional interventions aimed at restoring legitimacy, improving service delivery, and bridging trust deficits.

This approach is most visible in regions such as Left-Wing Extremism (LWE)-affected districts, the Northeast, and Jammu & Kashmir, where governance gaps have historically been exploited by insurgents to establish parallel systems. The new paradigm combines hard power (modernised forces, security operations) with soft power (development, rehabilitation, civic action), reinforced by administrative reforms and technology-enabled governance. The ultimate goal is not merely to suppress insurgency but to dismantle its ecosystem—physical, ideological, financial, and digital.

i. Targeted Development and Infrastructure Programmes

Development is now seen as a non-negotiable precondition for peace. Flagship programmes tailored to conflict-affected regions include:

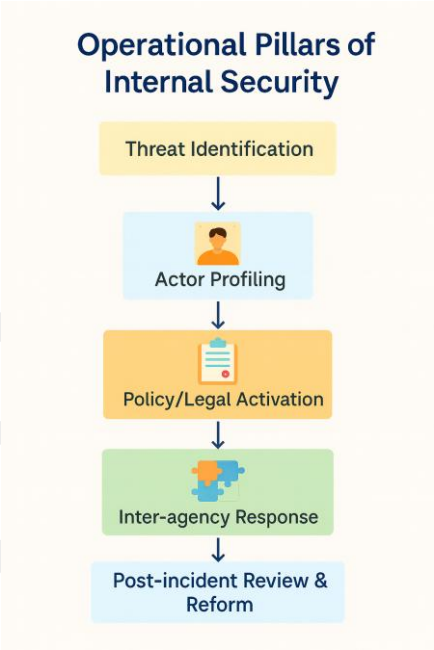
- **Aspirational Districts Programme (2018):** Covers 112 backward districts (many LWE-affected), focusing on health, education, financial inclusion, and infrastructure. Dashboards and rankings have driven improvement in districts like Bijapur (Chhattisgarh) and Malkangiri (Odisha).
- **Integrated Action Plan (IAP) / Special Central Assistance (SCA):** Provides untied funds to District Collectors for locally relevant projects (roads, irrigation, schools), reducing bureaucratic delays.
- **Core Infrastructure Initiatives:**
    - *PMGSY* for rural roads,
    - *BharatNet* for digital connectivity,
    - *Saubhagya* for electrification,

- *Jal Jeevan Mission* for piped water,
- Mobile towers under MHA packages for remote Maoist areas.

- **Van Dhan Yojana & Eklavya Model Schools:** Enhance tribal livelihoods and education, reducing vulnerability to extremist propaganda.

Where roads, schools, and banking penetrate, extremist influence demonstrably weakens.

ii. Security–Development Synergy Frameworks



- **Civic Action Programme (CAP):** CAPFs (CRPF, BSF, ITBP) conduct health camps, sports, and cultural events to humanise the forces. In Dantewada, football tournaments became a tool against Maoist recruitment.
- **SAMADHAN Doctrine (2017):** A comprehensive MHA framework combining:
  - Smart leadership through young officers,
  - Aggressive area domination,
  - Actionable intelligence (HUMINT, TECHINT, OSINT),
  - Technology adoption (UAVs, GIS mapping, mobile tracking),
  - Agency coordination via unified commands,
  - Denial of finances by cracking down on extortion and front NGOs.
- **Bastariya Battalion (CRPF):** Raised from local tribal youth in Bastar, ensuring cultural connect, terrain mastery, and local employment—building both representation and trust.

iii. Administrative and Technological Innovations

- **Posting of Young IAS/IPS Officers:** Energetic officers in conflict zones are given flexible funds and encouraged to engage directly with citizens through *Janata Darbars* and grievance apps.
- **Mobile Governance Tools:**
  - *e-Gram Swaraj* for panchayat fund tracking,
  - *Tele-Law* and *PMGDISHA* for legal literacy,
  - Geo-tagging of MGNREGA and IAP assets for transparency.
- **Emerging Tech Experiments:** Drones for mapping, surveillance, and even last-mile service delivery in remote areas.

iv. Confidence-Building and Perception Management

- **Surrender and Rehabilitation Policy:**
  - One-time financial grant (₹2.5–5 lakh),
  - Vocational training and safe housing,
  - Recruitment preference in Home Guards and MSMEs,
  - Legal protections for low-ranking cadres.
  - *Chhattisgarh's "Lone Varatu" campaign (2019–22)* led to 400+ Maoist surrenders.
- **Information and Perception Warfare:**
  - Community radio, folk art, and mobile vans spread awareness of welfare schemes.

    - Social media in local languages builds trust and counters propaganda.
- **Civic Empowerment:** CAPFs assist in Gram Sabha activities, ration card drives, and legal aid camps, helping reposition the state as a protector rather than predator.

v. Security Force Modernisation and Tactical Realignment

- **CRPF CoBRA Battalions:** Specialised in jungle warfare and guerrilla combat.
- **Greyhounds (Andhra Pradesh & Telangana):** Fast-reaction jungle units with high kill-to-loss ratio.
- **SOG & DRG (Chhattisgarh):** Tribal recruits trained in local intelligence and operations.
- **Joint Command Centres:** Integrate CRPF and state police for real-time operations.

Forces are increasingly equipped with IED detection tools, satellite navigation, and deep forest insertion training, reducing casualties and improving precision.

vi. Monitoring and Coordination Mechanisms

- **Unified Command Structures:** Coordinate IB, NIA, state police, and CAPFs at the state level.
- **Security & Empowerment Committees (SEC):** Balance development and policing reviews.
- **District Mineral Foundation (DMF):** Redirects mining royalties to tribal welfare.
- **MHA Dashboards:** Enable real-time monitoring of district-level progress, schemes, and officer performance.
- **CAPF Modernisation Funds:** Upgrade mobility, surveillance, and tactical equipment.

Conclusion

India's response to governance deficits has evolved from reactive policing to a calibrated, people-centric model. By combining targeted development, localised security, administrative reforms, and perception management, the state is gradually dismantling insurgent parallel systems and reducing extremist appeal.

The guiding philosophy is clear: *"Peace cannot be won by force alone—it must be earned through governance that delivers justice, dignity, and opportunity."*

As one Bastar civil servant observed: *"In conflict zones, a school built is a gun surrendered."* The true success of India's counter-insurgency strategy lies not only in suppressing violence but in embedding trust, legitimacy, and hope within vulnerable communities.

The diverse interventions—from infrastructure building and tech-enabled governance to rehabilitation and civic empowerment—highlight India's attempt to blend force with development and legitimacy.

Yet, to fully appreciate why LWE persists despite such efforts, one must examine its geographical heartland—the "Red Corridor." Stretching across central and eastern India, this belt has provided the terrain and social context for Maoist insurgency for decades. Analysing its geography, trends in violence, and shifting strongholds is essential to understand why some districts remain entrenched in conflict while others have stabilised.

2.8 Geography of the Red Corridor and Trends in Violence

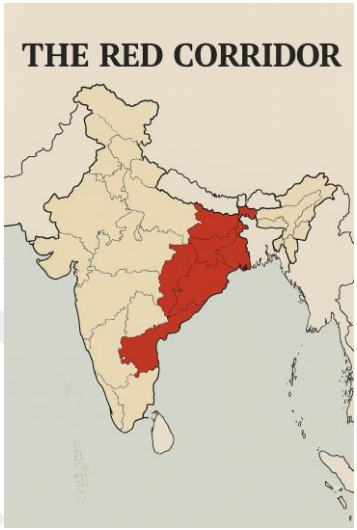
a. Introduction

The "Red Corridor" refers to the swathe of districts across central and eastern India historically affected by Left-Wing Extremism (LWE). Geographically, it cuts through tribal-dominated, forested, and mineral-rich belts, where displacement, exploitation, and weak governance created the vacuum in which Maoist mobilisation flourished. These structural vulnerabilities enabled insurgents not only to

mount armed resistance but also to establish parallel systems of authority, positioning themselves as alternative dispensers of justice and protection.

While sustained counter-insurgency operations and developmental programmes have substantially reduced the Maoist footprint, the insurgency has adapted rather than disappeared. Its geography has contracted into fewer strongholds, but its tactics, networks, and ideological fronts have evolved in ways that remain a persistent challenge. Mapping this spatial and operational evolution—particularly the division between core, buffer, and fringe areas—is essential to understand both the resilience and vulnerabilities of the movement.

b. Geographical Spread of the Red Corridor



Current LWE activity is concentrated in a handful of states:

- Chhattisgarh: Bastar, Sukma, Dantewada, Bijapur
- Jharkhand: Latehar, Gumla, Lohardaga, West Singhbhum
- Odisha: Malkangiri, Koraput, Kandhamal
- Maharashtra: Gadchiroli
- Bihar: Gaya, Aurangabad
- Andhra Pradesh & Telangana: Activity largely subdued, but forested border tracts remain sensitive

Among these, Bastar in southern Chhattisgarh is today considered the last major stronghold of the Maoists.

c. Mapping Maoist Influence: Core, Buffer, and Fringe

- **Core Areas:** Complete Maoist dominance, where state presence is minimal and security forces face formidable challenges. Example: Abujhmaad forests of Chhattisgarh, nearly 4,000 sq. km of unsurveyed terrain.
- **Buffer Zones:** Contested spaces where influence shifts depending on security deployments, governance penetration, and local sentiment.
- **Fringe Areas:** Districts once under Maoist sway but stabilised through combined security and development efforts, now gradually reintegrating into mainstream governance.

This three-tier mapping demonstrates how the insurgency survives by retreating deeper into forests while resisting state penetration in contested zones.

d. Current Patterns in Left-Wing Extremism

i. Tactical Consolidation into Forested Core Zones

The insurgency has shifted from widespread territorial control to concentrated guerrilla warfare in:

- Abujhmaad (Chhattisgarh) – un-surveyed, inaccessible forests
- Indravati–Godavari corridor (Chhattisgarh–Odisha–Maharashtra)
- Remote tracts of Malkangiri (Odisha) and Gadchiroli (Maharashtra)

This is a tactical fallback, consistent with guerrilla doctrine—conceding space to regroup in favourable terrain.

ii. Shift in Attack Modus Operandi

Earlier Tactics	Current Tactics
Mass ambushes on police convoys (e.g., Dantewada 2010, 76 CRPF killed)	Smaller, targeted IEDs, sniper fire, hit-and-run attacks

Earlier Tactics	Current Tactics
Political assassinations of local leaders	Reduced civilian targeting to avoid backlash; focus on security forces
Extortion of large corporations	Levies from rural contractors, forest-produce traders, welfare delivery systems

IEDs now account for over 60% of Maoist-related fatalities (2022–23), showing preference for low-cost, high-impact tactics.

iii. Increased Reliance on Tribals and Women Cadres

- With urban recruitment shrinking, Maoists rely heavily on tribal belts still marked by alienation.
- Women constitute 30–40% of cadres in some regions; children inducted into *Bal Sanghams* as informants and couriers.
- This ensures invisibility, cultural blending, and long-term grooming.

iv. Urban Naxalism and the Ideological Overground

- Even as rural zones shrink, Maoists cultivate urban support networks through universities, NGOs, rights groups, and digital media.
- Urban operatives act as "invisible generals"—handling funding, propaganda, legal defence, and media framing.
- The Bhima Koregaon case (2018) revealed encrypted communication and strategy documents linking activists with Maoist leadership.

v. Digital Tools, Encryption, and Propaganda

- Shift from couriers to encrypted platforms (*Telegram, Signal, custom apps*).
- Digitised manifestos in multiple languages, dark web channels, and WhatsApp propaganda campaigns.
- Content often highlights alleged state atrocities, aiming to radicalise and mobilise support.
- Yet, digital surveillance and cyber-forensics increasingly expose these networks.

vi. Micro-Economies and Welfare Sabotage

- Maoists now depend on steady local revenue streams rather than big corporate levies.
- Targets include MNREGA supervisors, PDS networks, and small contractors.
- Sabotage of welfare projects (roads, mobile towers, Anganwadi centres) prevents the state from consolidating legitimacy.
- Parallel taxation of tendu leaf and bamboo traders sustains a shadow economy.

vii. Public Disillusionment and Leadership Crisis

- Greater access to education, telecom, and welfare has eroded Maoist appeal in some villages.
- 2,000+ cadres surrendered in five years, aided by schemes like *Lone Varatu* (Chhattisgarh).
- Leadership faces generational fatigue: ageing commanders disconnected from grassroots realities, struggling to inspire new recruits.

Conclusion

The Maoist insurgency has transitioned from a territorial rebellion into a fragmented, covert, and ideologically-driven movement. Its tactical reliance on IEDs, digital propaganda, tribal recruitment, and micro-economies reflects adaptation—but also reveals vulnerabilities in the face of expanding governance, education, and surveillance.

As NSA Ajit Doval observed: *"You cannot shoot an ideology; you have to expose its hollowness."* Neutralising Maoism therefore requires more than counter-insurgency; it demands delegitimising its ideological appeal while ensuring governance delivers dignity, justice, and opportunity.

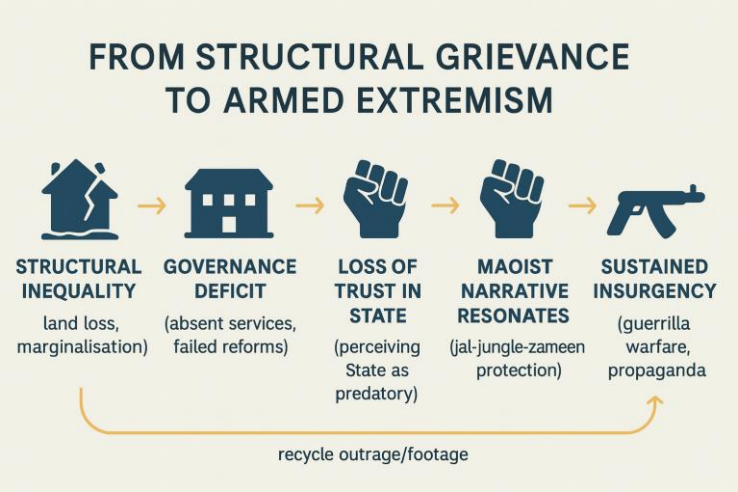
The evolving geography and tactics of LWE show why it has endured despite decades of security and development interventions. Its persistence is rooted not only in strategy but in structural grievances—land alienation, displacement without rehabilitation, and tribal marginalisation—that insurgents continue to exploit.

To move beyond containment towards resolution, it is essential to examine these structural causes of LWE at the intersection of governance, justice, and socio-economic inequality—the subject of the next section.

2.9 Structural Causes of Left-Wing Extremism (LWE)

a. Introduction

Left-Wing Extremism (LWE), popularly associated with Naxalism or the Maoist insurgency, is one of India's most enduring internal security challenges. Rooted in Marxist–Leninist–Maoist ideology, it seeks to overthrow the Indian state through protracted armed struggle, mobilising the rural poor, tribals, and landless peasants. Unlike external aggression or religious extremism, Maoism is indigenous and class-based, deriving legitimacy from structural inequalities: landlessness, displacement, exploitation of natural resources, and the alienation of marginalised communities.



Its appeal lies not merely in ideology but in its resonance with lived experience. For many in tribal belts, the promise of "jal–jungle–zameen" (water, forest, land) resonates more deeply than the abstractions of state-led development. The movement has thrived wherever structural deprivation and governance apathy created a vacuum, allowing insurgents to pose as protectors of the dispossessed. LWE is thus not only a security problem but also a developmental and governance crisis.

b. The Naxal Movement: Origins and Evolution

- **1967 – Naxalbari Uprising (West Bengal):** Led by Charu Mazumdar and Kanu Sanyal, peasants revolted against landlords, marking the birth of the Naxalite movement.
- **1970s–1990s:** Expanded across rural belts, especially in Andhra Pradesh, Bihar, and Jharkhand, drawing strength from agrarian inequality.
- **2004:** Formation of the Communist Party of India (Maoist) through the merger of People's War Group (PWG) and Maoist Communist Centre (MCC), consolidating the insurgency.
- **2000s:** At its peak, Maoists controlled vast swathes of the "Red Corridor."
- **2010s onwards:** Decline in territorial control due to security operations, yet tactical adaptation into asymmetric guerrilla warfare, digital propaganda, and urban ideological networks.

c. Strategic Relevance

The Maoist challenge cuts to the heart of India's democratic legitimacy—raising fundamental questions about tribal rights, land justice, and resource governance. It undermines state authority in some of the country's richest mineral belts, where governance is weakest.

- The Ministry of Home Affairs (MHA) notes a sharp decline in violence and affected districts (from 223 in 2008 to 45 in 2023).
- Yet, the ideological and operational threat persists, especially in parts of Chhattisgarh, Jharkhand, Odisha, and Maharashtra.
- As E. N. Rammohan, former DG of BSF, observed:
  "Maoism is not merely an armed movement. It is a symptom of our developmental failure, our administrative apathy, and our inability to build a just and inclusive state."

d. Core Structural Causes of LWE

i. Land Alienation and Forest Displacement

- Tribals often lack formal titles under the Forest Rights Act (2006).
- Mining, dams, and Special Economic Zones (SEZs) displace communities without timely rehabilitation.
- Maoists exploit this dispossession, projecting themselves as defenders of jal–jungle–zameen.
- *Example:* Resistance to Vedanta's bauxite mining in Niyamgiri and POSCO's steel project in Odisha drew heavily on Maoist narratives.

ii. Historical Exploitation by State Agents

- Forest officials, police, and contractors have long exploited tribal communities through harassment, illegal fines, and corruption.
- Custodial violence and arbitrary arrests foster resentment.
- Maoist-run Jan Adalats (people's courts) gain legitimacy by offering swift—if brutal—justice.

iii. Development Deficit in Basic Services

- Conflict zones lack schools, health centres, all-weather roads, electricity, and telecom.
- Poverty and joblessness provide a steady recruitment pool for insurgents.
- The overlap of NITI Aayog's Aspirational Districts with LWE areas underscores the development–security nexus.

iv. Breakdown of Trust in Governance

- Officials rarely visit interior villages; funds are siphoned off or projects abandoned under Maoist threats.
- Grievance redress is absent, driving locals to insurgents for dispute resolution and crisis support.
- This erodes state legitimacy and entrenches parallel governance.

v. Identity-Based Marginalisation

- Tribals, SCs, and OBCs remain under-represented in civil services, judiciary, and local governance.
- Ignoring tribal customs, dialects, and traditional institutions fuels emotional and political alienation.

vi. Failure of Land Reforms and FRA Implementation

- The Forest Rights Act (2006) intended to empower forest dwellers, but:
  - Claims often rejected,
  - Bureaucratic harassment persists,
  - Lack of legal literacy leaves many excluded.
- Such failures turn a law of empowerment into a source of frustration, reinforcing Maoist propaganda.

vii. Economic Exploitation in Mineral-Rich Zones

- Resource-rich belts contain iron ore, bauxite, coal, manganese.

- Mining projects displace communities without benefits; profits bypass locals.
- Pollution and land loss generate resentment—a classic "resource curse" that insurgents weaponise.

viii. Ineffective Implementation of Welfare Schemes

- Flagship programmes—PDS, MGNREGA, pensions—falter due to corruption, poor monitoring, or Maoist disruption.
- Weak banking and digital infrastructure compound exclusion.
- Locals perceive neglect as betrayal, while Maoists step in with promises of fairness.

As one civil servant aptly remarked: *"Extremism doesn't begin with a gun; it begins with a grievance. If the grievance is just, the gun follows soon."*

Conclusion

Left-Wing Extremism is not merely a military threat; it is a reflection of India's unfinished agenda of justice, inclusion, and equitable development. Land alienation, cultural exclusion, failed welfare delivery, and exploitative state–citizen relations have provided Maoists with enduring moral ground.

Security operations may suppress insurgency, but unless these systemic injustices are addressed, the movement will retain ideological space. The fight against LWE must therefore be waged not only with guns, but also with land titles, functioning schools, accessible healthcare, and accountable governance.

As counterinsurgency pioneer K. P. S. Gill observed: *"You cannot kill an idea with a bullet. You can only kill it with a better idea."*

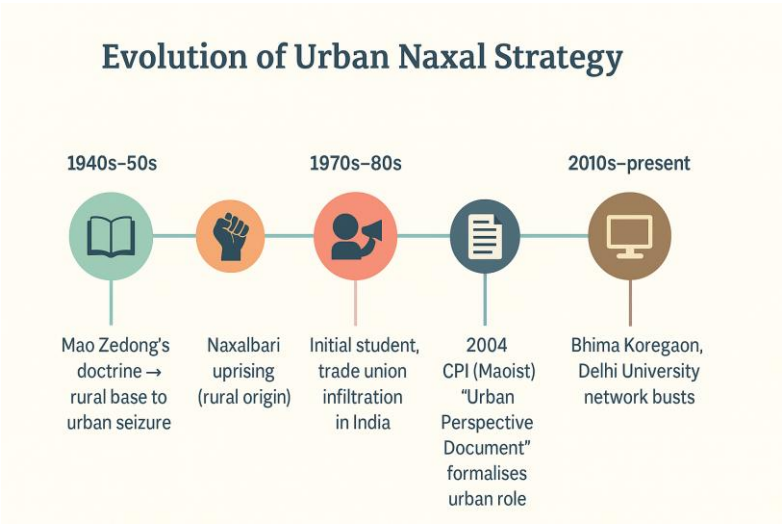
While structural causes explain why LWE found deep roots in India's tribal belts, its persistence cannot be explained by rural grievances alone. Over time, Maoism has drawn sustenance from an urban ecosystem of intellectuals, activists, NGOs, and digital networks. This phenomenon—often termed Urban Naxalism—serves as the ideological engine of the insurgency, providing legitimacy, legal defence, propaganda, and recruitment channels even as armed wings shrink.

The next section will therefore turn to Urban Naxalism, analysing its nature, networks, and impact on the broader Maoist movement.

2.10 Rise of Urban Naxalism: Ideological Engine of Left-Wing Extremism

a. Introduction

Urban Naxalism represents the ideological, intellectual, and logistical face of Left-Wing Extremism (LWE) in India. Unlike armed cadres in forests who directly engage in insurgency, Urban Naxals operate from within civil society spaces—universities, courts, media, NGOs, cultural forums, and professional associations.



The term, though controversial, broadly refers to individuals and networks who:

- Justify or romanticise Maoist violence,

- Act as sympathisers or facilitators,
- Provide legal and financial aid,
- Craft narratives that delegitimise the state while framing insurgency as "people's resistance."

Their contribution is less about combat and more about sustaining the ecosystem of insurgency. Through advocacy, propaganda, and support networks, Urban Naxals ensure that the Maoist struggle retains intellectual legitimacy, urban recruitment, and operational lifelines—even as rural strongholds shrink under security pressure.

b. Historical Roots of the Urban Strategy

The Maoist use of urban operatives is not accidental; it is strategically embedded in classical doctrine. Mao Zedong emphasised that revolution must grow from rural bases to ultimately encircle and capture cities.

This philosophy found explicit articulation in the "Urban Perspective Document" (2004) of the Communist Party of India (Maoist), which calls for systematic infiltration of:

- Student movements and universities – to mobilise disillusioned youth.
- Labour unions and worker associations – to build an industrial base for agitation.
- Civil liberties groups and NGOs – to cloak insurgent networks under rights-based activism.
- Cultural platforms and media spaces – to romanticise the insurgency as people's revolution.

These nodes are tasked with creating shelter networks, propaganda channels, and funding pipelines, while shaping public discourse in ways that weaken the legitimacy of the Indian state.

c. Strategic Functions of Urban Naxals

i. **Ideological Justification**

- Frame Maoist violence as legitimate resistance against oppression.
- Publish pamphlets, books, and seminar papers portraying insurgency as "class struggle."

ii. **Recruitment and Radicalisation**

- Universities and urban youth hubs serve as fertile ground.
- Narratives of caste oppression, tribal rights, displacement, and state repression are used to mobilise support.

iii. **Legal and Logistical Support**

- Provide legal aid to arrested cadres.
- Maintain safe houses, organise couriers, and facilitate transit routes under the guise of rights advocacy.

iv. **Propaganda and Narrative Management**

- Highlight custodial deaths, fake encounters, or displacement as evidence of "state oppression."
- Use exaggerated or selective accounts to delegitimise counter-insurgency operations.

v. **Financial Facilitation**

- Use NGOs, cultural forums, and academic grants to pool and redirect funds.
- Some networks channel foreign donations into extremist-linked activities.

vi. **Intelligence and Communication**

- Act as conduits between rural cadres and external supporters.
- Employ encrypted platforms (Signal, Telegram, custom apps) to maintain operational secrecy.

d. Symbiosis Between Rural Maoists and Urban Naxals

Rural Maoists	Urban Naxals
Engage in armed insurgency in forest belts	Provide ideological and strategic guidance from cities
Depend on tribal recruits	Depend on educated elites, activists, and sympathisers
Conduct ambushes, run "Jan Adalats"	Host university debates, publish NGO reports, mobilise protests
Exercise physical warfare	Wage intellectual and narrative warfare

The relationship is mutually reinforcing: rural insurgents rely on urban nodes for legitimacy and resources, while urban networks derive purpose from the existence of armed struggle. Together, they form a hybrid insurgency that combines the gun and the pen.

e. High-Profile Cases and Investigations

i. Bhima Koregaon Case (2018)

- Arrests of activists and academics on charges of inciting caste violence during the bicentenary of the Bhima Koregaon battle.
- Investigations alleged links to Maoist organisations, conspiracy to assassinate the Prime Minister, and circulation of strategy documents advocating large-scale violence.

ii. Delhi University Network

- Professors and intellectuals from premier institutions were accused of connections with banned extremist groups.
- Cases highlighted how academic spaces doubled as platforms for ideological dissemination and recruitment.

iii. Urban Network Busts

- The NIA and state police have uncovered safe houses, courier networks, and financial pipelines in Pune, Hyderabad, and Delhi.
- These operations revealed the depth of Maoist infiltration into civil society domains.

f. Tools and Methods Used by Urban Naxal Networks

Urban Maoist sympathisers rely on sophisticated, adaptive techniques to sustain their networks. These tools range from encrypted technologies to narrative subversion, allowing them to operate under the cover of legality while sustaining insurgency in rural belts.

- **Encrypted Communication**
  Secrecy is the bedrock of underground operations. Urban Maoists rely on encrypted applications such as Signal, Briar, Telegram, and Threema. Dark web forums and TOR browsers provide further anonymity. Even traditional letters or emails often use coded language—for instance, an upcoming "concert" may actually refer to a planned armed ambush.
- **Digital Propaganda**
  The digital ecosystem is exploited as a force multiplier. Vernacular e-magazines, manifestos, and videos circulate widely among students and activists. YouTube channels, blogs, and WhatsApp groups push narratives glorifying Maoist ideology. Hashtag campaigns are often orchestrated immediately after encounters, discrediting security forces and shaping perceptions before official clarifications reach the public.
- **Ideological Subversion**
  Urban sympathisers embed themselves within legitimate platforms of dissent—student

unions, Dalit organisations, tribal rights forums. They organise seminars, film screenings, and lectures that reframe Maoist ideology as a form of social justice. Historical grievances like caste discrimination and displacement are reinterpreted as revolutionary legitimacy.

- **Legal and Judicial Aid**
  "Lawfare" has become central to sustaining the urban network. Civil liberties groups extend free legal aid to accused Maoists. Public Interest Litigations and RTI applications are deployed to stall investigations. Arrested individuals are projected as "political prisoners," converting courtrooms into propaganda platforms.
- **Financial Support**
  Urban networks serve as conduits for resource mobilisation. NGO fronts and loopholes in the Foreign Contribution Regulation Act (FCRA) enable the inflow of foreign grants. Crowdfunding platforms and donor networks generate additional funds. These are channelled to rural cadres via hawala networks and cash couriers, ensuring continuity of operations in conflict zones.
- **Narrative and Media Control**
  Information warfare is a core strategy. Sympathetic journalists, bloggers, and intellectuals amplify Maoist perspectives in mainstream debate. Articles and television panels often question the legitimacy of counter-insurgency operations. Social media campaigns (#FreePoliticalPrisoners, #FakeEncounter) generate moral pressure on state institutions, complicating enforcement.

g. Urban versus Rural Naxal Tools and Tactics

Dimension	**Urban Naxals – *The Nervous System***	**Rural Maoists – *The Muscle***
Primary Role	Ideological, financial, legal, and narrative support	Armed insurgency and tactical operations
Weapons Used	Pen, law, technology, and media	Guns, IEDs, and landmines
Communication	Encrypted apps, dark web, email	Couriers, jungle meetings, coded signals
Recruitment Base	University students, NGOs, disaffected urban youth	Tribal youth, displaced peasants, marginalised villagers
Propaganda Method	Social media, YouTube, academic lectures, journals	Posters, pamphlets, village meetings
Institutional Infiltration	Academia, NGOs, legal system, rights platforms	Panchayats, forest institutions, tribal councils
Funding Source	Urban donors, NGO/FCRA channels, crowdfunding	Extortion, taxation of forest produce, rural levies
Legal Status	Operates openly under cover of activism	Declared illegal under UAPA, underground
Operational Strategy	Narrative subversion, legal cover, resource channelling	Ambushes, assassinations, sabotage of state projects
Visibility	High-profile, in plain sight of media and institutions	Low-profile, embedded in hostile forest terrain

In Maoist doctrine, the logic is clear: *"the guerrilla must move amongst the people as a fish swims in the sea."* Rural cadres form the body of the movement, while urban operatives form its nervous system—providing ideology, legitimacy, and critical linkages.

Conclusion

Urban Naxalism may not wield guns, but it is equally vital to the Maoist ecosystem. By offering intellectual justification, legal cover, propaganda channels, and financial support, it shields the insurgency from complete eradication.

Confronting this challenge requires a delicate balance—ensuring that genuine dissent and activism are not stifled, while maintaining vigilance against covert subversion disguised as civil rights advocacy.

As one analyst aptly put it: *"Urban Naxalism is the invisible nervous system that fuels the muscle of rural Maoist insurgency."*

The rise of Urban Naxalism highlights how Maoism has survived through a dual structure—rural armed struggle and urban ideological advocacy. Together, they complicated India's counter-insurgency responses. Yet, despite these challenges, the state has achieved considerable success in rolling back Left-Wing Extremism over the past two decades. The shrinking geography of violence, declining cadre strength, and greater community participation in governance reflect tangible progress.

It is therefore necessary to now assess the achievements and milestones of India's strategy against LWE, to understand how far the country has come in dismantling one of its most enduring internal security threats.

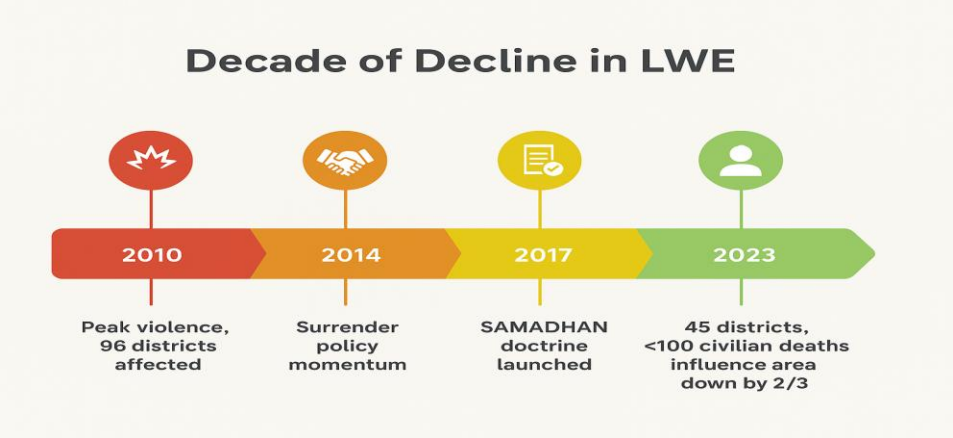
2.11 Achievements So Far in Tackling Left-Wing Extremism

a. Introduction

The Indian State's campaign against Left-Wing Extremism (LWE) has undergone a remarkable transformation over the past two decades. What began as a largely reactive, force-centric counterinsurgency has matured into a strategic, multi-layered mission that simultaneously targets the insurgency's armed strength, ideological appeal, and socio-economic roots.

Since 2010—particularly with the adoption of the SAMADHAN doctrine and the Aspirational Districts Programme (ADP)—India's approach has integrated security operations with infrastructure development, tribal empowerment, digital penetration, and community engagement. This paradigm shift has generated measurable outcomes: a sharp decline in violence, the visible expansion of governance into previously ungoverned spaces, and a perceptible change in community attitudes.

The synergy between central armed police forces (CAPFs), state police, local administrations, and tribal youth participation has been the defining feature of this success story.



b. Quantitative Achievements

Data from the Ministry of Home Affairs and the Press Information Bureau illustrates the scale of change:

Metric	2010	2023	Improvement
LWE-affected districts	96	45 (25 most affected)	Reduced by over 50%
LWE-related incidents	~2,258	~391	Decline of ~80%
Civilian deaths (annual)	720+	<100	Decline of >85%
Security force fatalities	300+	<30	Decline of ~90%
Area under Maoist influence	~60,000 sq km	<20,000 sq km	Decline of nearly 67%
Surrenders (2014–2023)	–	3,000+ cadres	Mass disengagement from insurgency

These numbers confirm the shrinking footprint of Maoist activity and a strengthened state presence in regions once considered ungovernable.

c. Governance Penetration Achievements

The true transformation lies not only in security metrics but in the expansion of governance into areas where Maoists once monopolised authority:

- **Road Connectivity:** Over 10,000 km of rural roads built in LWE zones under PMGSY since 2015, enabling both state penetration and economic opportunity.
- **Telecom Infrastructure:** 4G mobile towers installed in Sukma, Dantewada, Gadchiroli, and Malkangiri, converting former "communication black holes" into connected regions.
- **Banking Access:** Mobile ATMs and Common Service Centres (CSCs) now operate in over 200 Maoist strongholds, advancing financial inclusion.
- **Education:** Over 500 Eklavya Model Residential Schools sanctioned for tribal youth, reducing ideological vulnerability.
- **Digital Connectivity:** BharatNet has extended fibre-optic access to more than 13,000 Gram Panchayats in red-zone states.

This infrastructural push has delivered a visible state presence, weakening Maoist claims of being the "only authority" in remote belts.

d. Qualitative Achievements

Beyond the numbers, subtle but decisive shifts have occurred in the psychology of conflict:

- **Perception Change:** Tribal communities increasingly demand welfare services, roads, and schools, rejecting Maoist isolationist narratives.
- **Cadre Fatigue:** Maoist ranks are ageing and disillusioned, with declining recruitment among youth.
- **Localised Security Models:** Initiatives like the District Reserve Guards (DRG) and Bastariya Battalion showcase the success of "security by locals, for locals."
- **Youth Engagement:** Sports tournaments, cultural events, and vocational programmes have created non-militant identities for tribal youth.
- **Narrative Contestation:** The State now actively counters Maoist propaganda in both digital and physical spaces, ensuring insurgents no longer dominate the information war.

Conclusion

India's achievements against Left-Wing Extremism reflect the power of a calibrated, development-centric, and people-driven strategy. Violence has plummeted, governance has expanded into once-inaccessible villages, and communities increasingly demand education, jobs, and dignity instead of jungle justice.

Yet the battle is not over. Maoist ideology, though weakened, retains pockets of influence—sustained by structural grievances, difficult terrain, and ideological networks. As the Ministry of Home Affairs cautions: *"The decline of violence does not mark the end of the war—it signals the start of winning hearts."*

The measurable decline in violence and the steady penetration of governance are undeniable. But these gains coexist with stubborn obstacles—the Maoists' adaptability, their use of terrain, persistent governance deficits, and ideological survival through urban networks. To make progress irreversible, it is crucial to assess the persistent challenges that continue to impede the full transformation of conflict zones into secure and developed regions.

The next section therefore examines these enduring challenges in tackling LWE.

2.12 Persistent Challenges in Tackling Left-Wing Extremism

a. Introduction

Even as India has decisively weakened Left-Wing Extremism (LWE)—shrinking its footprint, reducing violence, and expanding governance into once-inaccessible zones—the final frontier remains the most complex. Like many asymmetrical conflicts, the Maoist insurgency has adapted to survive in hardened forest terrains, cyber spaces, and urban ideological fringes.

What now persists are not vast liberated zones but fragmented strongholds fortified by geography, mistrust, and narrative warfare. Eliminating this last-mile challenge requires more than force; it demands surgical precision, cultural sensitivity, and post-conflict reconciliation.

The following challenges highlight why the Maoist threat, though diminished, is not yet extinguished.

i. Resilient Maoist Strongholds

Certain geographies remain virtually ungoverned. The Abujhmaad forest in Chhattisgarh, still unsurveyed and hostile to state entry, is emblematic of this challenge. Similar hardened pockets exist in the Odisha–Chhattisgarh–Maharashtra tri-junction, southern Bastar, and parts of Gadchiroli.

In these enclaves, Maoists continue to run parallel systems of governance—conducting "people's courts," levying taxes, and patrolling villages—thereby maintaining the illusion of sovereignty.

ii. Operational Coordination Gaps

Despite improvements, counter-LWE operations remain fragmented. Central Armed Police Forces (CAPFs) and state police units often act without full integration, leading to duplication and delayed responses.

Intelligence from the Intelligence Bureau (IB) and National Investigation Agency (NIA) is not consistently shared in real time, reducing pre-emptive effectiveness. Jurisdictional overlaps between NIA, Anti-Terrorism Squads, and Special Branches further create confusion, eroding the tactical edge.

This "security siloing" undermines operational superiority, even when force strength is considerable.

iii. IED Warfare and Tactical Adaptation

The Maoists' ingenuity in low-cost, high-impact weaponry continues to inflict disproportionate damage. Improvised explosive devices (IEDs) account for more than 60 percent of LWE-related casualties.

- Pressure-plate mines under village roads
- Claymore devices on jungle routes
- Sniper nests in trees

These tactics turn terrain into a constant hazard. They make mobility risky and constrain security forces to defensive caution, slowing the pace of operations.

iv. Tribal Mistrust and Alleged Police Excesses

The battle against Maoism is as much about perception as about force. Heavy-handed policing, alleged fake encounters, and staged surrenders have created a lingering trust deficit.

Delays in justice delivery compound the problem, allowing Maoist propaganda to portray the state as exploitative. As one villager starkly put it: *"The State is not cruel like Maoists, but neither is it very kind."*

v. Development Implementation Gaps

Physical penetration of the state has not always translated into performance. Development funds often go unspent, as contractors withdraw under Maoist threats.

- Corruption and leakages plague flagship schemes such as the Public Distribution System (PDS) and MGNREGA.
- Manpower shortages—doctors, teachers, engineers—cripple service delivery in remote districts.
- Digital divides further hinder welfare outreach.

Presence without efficiency becomes an empty shell, one easily exploited by insurgent narratives.

vi. The Urban Naxal Narrative

While rural violence declines, the ideological war has shifted to cities. Sympathisers in academic, legal, and activist circles frame Maoist violence as revolutionary struggle, while painting counter-insurgency operations as state oppression.

- Funding, legal cover, and narrative support flow through these urban networks.
- Digital platforms amplify propaganda, framing the conflict as "bullet versus blog."

This underlines that the insurgency survives not only in forests but also in the discourse of dissent.

vii. Gaps in Post-Surrender Rehabilitation

Surrendered cadres, while counted as a statistical success, often find themselves in limbo.

- Many face unemployment, social stigma, and lack of skills, making reintegration difficult.

- Others face threats of reprisal from hardline Maoists, leaving them vulnerable.

In the absence of credible livelihood opportunities and social acceptance, some drift back into extremism or fall prey to other criminal networks.

Conclusion

India's struggle against Left-Wing Extremism has entered a decisive but delicate phase. The insurgency is no longer an existential threat to the state, but its residual embers—rooted in terrain, mistrust, and ideology—retain the potential to reignite sporadic violence and popular alienation.

To secure irreversible peace, the state must transition from reactive containment to proactive consolidation. This requires:

- Building tribal trust through rights-based governance.
- Ensuring last-mile delivery of development.
- Countering urban propaganda.
- Providing dignity-centred rehabilitation to surrendered cadres.

Long-term peace in the Red Corridor will not be declared from a CRPF outpost; it will be visible in a child attending school without fear, in an ex-Maoist finding dignified employment, and in a village where the state is seen as protector rather than predator.

As E.N. Rammohan, former Director General of the Border Security Force, once reminded: *"You can never win hearts by chasing shadows in forests. You win them by lighting a lamp in every neglected home."*

The persistent challenges of LWE, as seen in hardened strongholds and governance vacuums, often appear abstract when discussed at the national level. Yet, the real impact of this conflict—and the true test of state response—unfolds in specific districts where lives, livelihoods, and legitimacy are contested daily.

Among these, Dantewada and Sukma in Chhattisgarh's Bastar region stand out as emblematic battlegrounds. These districts are not just geographical spaces but living laboratories of the LWE conflict—dense forests that shelter guerrilla strongholds, tribal communities caught in the crossfire, and state institutions struggling to balance force with welfare.

By turning to Dantewada and Sukma, we move from theory to lived reality. They illustrate how structural grievances, tactical Maoist adaptations, and state interventions converge in complex ways. These case studies highlight both the scale of human suffering and the innovative attempts to reclaim ground, making them essential to any holistic grasp of India's battle against Left-Wing Extremism.

2.13 Case Studies: Dantewada and Sukma

a. Introduction

Case studies offer a lens into the lived realities of Left-Wing Extremism (LWE), revealing how local contexts shape both the persistence of violence and the state's capacity to respond. Dantewada and Sukma, located in Chhattisgarh's Bastar division, illustrate two contrasting trajectories: one of innovative outreach and perception management, the other of tragic failure in coordination and tactical preparedness.

Together, they underscore the complexity of counter-LWE efforts, where victories are hard-earned and setbacks carry heavy costs.

i. Dantewada, Chhattisgarh – The "Lone Varatu" Campaign

Period: 2019–2023
Theme: Surrender strategy and perception management

Dantewada has long been regarded as the symbolic heartland of Maoist insurgency. For decades, it witnessed deadly IED attacks, ambushes, and routine disruption of governance, with state presence largely confined to highways and fortified CRPF camps. In this difficult environment, conventional counter-insurgency yielded limited results, prompting an alternative approach rooted in emotional and cultural resonance.

The district police launched the "Lone Varatu" campaign, meaning *"Come Back Home"* in the local Gondi dialect. Instead of treating lower-rung Maoist cadres solely as criminals, the campaign reframed them as estranged family members, appealing to community ties and personal dignity.

Outreach was conducted through wall posters, folk songs, and personalised communication. The names of local youth involved in Maoist activity were publicly displayed—accompanied not by threats but by an offer of amnesty and rehabilitation.

Outcome:

- Over 400 Maoist cadres, including many women and minors, surrendered between 2019 and 2022.
- The district saw a marked reduction in recruitment and IED attacks.
- The initiative earned recognition from the Ministry of Home Affairs and was lauded in Parliament as a model framework for surrenders.

Dantewada's experience demonstrated that insurgency can be weakened not just through firepower but also through cultural narrative and trust-building, offering a rare example of perception management succeeding where policing alone had struggled.

ii. Sukma, Chhattisgarh – The 2021 Ambush and Coordination Failures

Period: April 2021
Theme: Operational lapses and leadership loss

Just 100 kilometres from Dantewada, Sukma remains one of the most volatile theatres of Maoist violence. In April 2021, a joint team of nearly 1,700 personnel drawn from the CRPF, District Reserve Guards (DRG), and the elite CoBRA unit launched an operation based on intelligence that top Maoist commander Madvi Hidma was present in the area between Tarrem and Silger.

The operation, however, revealed the continuing fragility of counter-insurgency coordination. The Maoists deliberately fed disinformation and used the difficult terrain to their advantage, luring the forces into an L-shaped ambush. The hilly and forested terrain, coupled with inadequate local intelligence support, left the security personnel exposed.

Impact:

- Twenty-three security personnel were killed, making it one of the deadliest attacks in recent years.
- Fourteen sophisticated weapons were looted by the Maoists.
- Post-mortem analysis revealed gaps in terrain familiarity, overreliance on drone-based intelligence, and insufficient integration of tribal informants into planning.

The Sukma incident became a stark reminder that sheer numbers and high-tech assets cannot substitute for micro-terrain knowledge, real-time human intelligence, and tight inter-agency coordination.

Conclusion

Taken together, Dantewada and Sukma illustrate two contrasting faces of India's counter-LWE struggle. Where Dantewada shows the promise of community engagement and narrative framing in eroding insurgent legitimacy, Sukma reflects the continuing dangers of underestimating Maoist adaptability and the unforgiving nature of forest warfare.

These cases emphasise that India's long-term success will depend on sustaining innovative soft-power strategies while simultaneously refining hard-power tactics.

The contrasting experiences highlight both the strengths and the vulnerabilities of India's counter-LWE efforts. On one hand, innovative campaigns like Lone Varatu demonstrate the power of perception management and community-led rehabilitation in dismantling insurgent influence. On the other, operational lapses in Sukma reveal the continued fragility of inter-agency coordination, terrain intelligence, and tactical preparedness.

These dual realities raise a larger question: How effective, balanced, and sustainable is India's overall strategy against Left-Wing Extremism?

A critical evaluation is therefore essential to understand not just what has worked, but also where the gaps persist—and how the approach can evolve into a truly long-term solution.

2.14 Critical Evaluation of India's Strategy Against Left-Wing Extremism

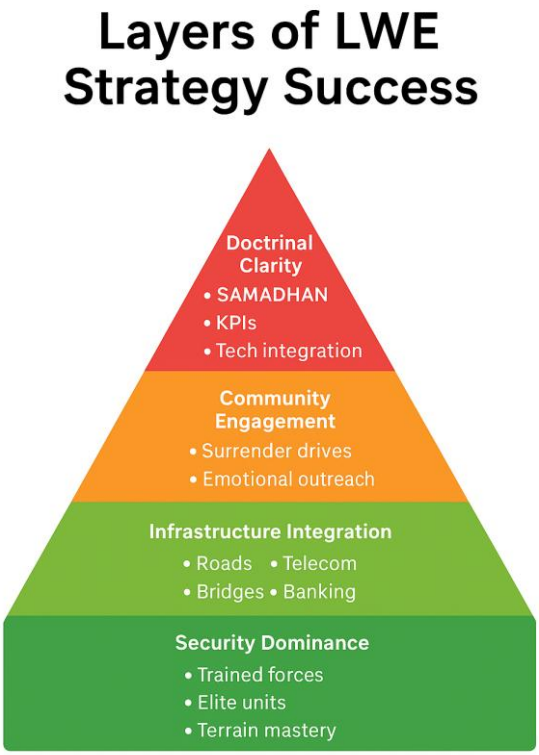
a. Introduction

India's response to Left-Wing Extremism (LWE) has undergone a steady transformation. What began as a force-dominated and reactive approach has evolved into a multi-dimensional framework that integrates security, development, rehabilitation, and governance.

The adoption of doctrines like SAMADHAN, modernisation of Central Armed Police Forces (CAPFs), infrastructure expansion in tribal belts, and community-focused initiatives has produced measurable results on the ground.

Yet, despite significant territorial and tactical gains, the movement has not been fully eradicated. Pockets of hardcore resistance remain, and Maoist influence now extends into less visible spaces such as digital platforms and urban intellectual networks.

This makes a critical evaluation of India's strategy essential—acknowledging both successes and limitations, and identifying the path forward.



b. What Has Worked Well

i. Sharp Decline in Violence and Spread

The most visible achievement is the steep reduction in Maoist violence and territorial influence:

- LWE-affected districts have declined from 96 in 2010 to 45 in 2023.
- Annual incidents have fallen from over 2,200 to fewer than 400.
- Civilian deaths have reduced from 700+ to under 100, and security force fatalities from 300+ to less than 30.

This reflects the strategic dominance of the state across much of the Red Corridor.

ii. Evolution of Strategic Thinking – SAMADHAN

The Ministry of Home Affairs introduced the SAMADHAN doctrine, which clearly articulated a hybrid strategy combining hard and soft measures. It integrated dashboard-based monitoring, technological

upgrades, and coordinated operations—shifting the focus from reactive policing to pre-emptive area domination.

iii. Infrastructure-Led Integration

Expansion of roads, telecom, banking, and power has disrupted Maoist logistics and reduced their capacity to isolate local communities.

- A symbolic example is the Gurupriya Bridge in Odisha's Malkangiri, which ended 15 years of Maoist dominance by physically linking isolated populations to state institutions.

iv. Community Engagement and Surrender Campaigns

Initiatives like "Lone Varatu" in Dantewada demonstrated the effectiveness of cultural and emotional messaging. Hundreds of cadres surrendered under this campaign, showing that trust-building can succeed where firepower alone falters.

v. Elite Forces and Localised Policing

Specialised forces such as the Greyhounds in Andhra Pradesh, the District Reserve Guards (DRG), and the Bastariya Battalion have revolutionised counter-insurgency. Their ability to adapt to terrain, recruit tribals, and respond quickly has sharply reduced the operational advantage once enjoyed by Maoists.

c. What Has Not Worked – Persistent Gaps

i. Hardcore Strongholds Remain

Zones such as Abujhmaad in Chhattisgarh and the Indravati–Godavari belt remain effectively inaccessible. Maoists continue to run parallel governance, holding people's courts and levying taxes.

ii. Coordination Deficits and Bureaucratic Fragmentation

Despite improvements, intelligence and operational silos persist:

- CAPFs and state police often function under dual command, creating confusion.
- IB and NIA intelligence is not consistently shared in real time.
- SOPs overlap across NIA, state ATS, and Special Branches.

The absence of a Unified Intelligence Grid hampers tactical superiority.

iii. Weak Execution of Welfare Schemes

Infrastructure has expanded, but service delivery remains fragile:

- Funds for MGNREGA, PDS, PMAY, and the Forest Rights Act are poorly implemented.
- Corruption, Maoist reprisals, and manpower shortages—especially of doctors and teachers—limit actual impact.

Thus, the state risks being present but ineffective, a vulnerability Maoists exploit.

iv. Evolving Maoist Tactics

Maoists have adapted by relying on IEDs, now accounting for over 60% of fatalities. They also strengthen their ideological base through urban networks that provide legal, financial, and propaganda support.

This "battle of narratives" continues to dilute the state's legitimacy.

v. Rehabilitation Gaps

While surrender campaigns show success, post-surrender reintegration remains weak:

- Skill training is delayed, job placements scarce, and cadres face reprisals or stigma.
- Without dignity and livelihood, rehabilitation risks becoming a revolving door back into extremism.

vi. Ethical and Legal Concerns

The extensive use of UAPA and slow trials raise questions about due process. Labelling dissenters as "Urban Naxals" without clear evidence dilutes legitimacy.

- High-profile cases, such as the arrest of Father Stan Swamy, attracted international criticism and weakened India's moral narrative.

d. SWOT Analysis of India's LWE Strategy

Dimension	Strengths	Weaknesses
Security Strategy	Specialised forces, doctrine clarity, tech adoption	Intelligence silos, patchy dominance in terrain
Development Approach	Roads, telecom, schools, Aspirational Districts	Corruption, manpower shortage, weak service delivery
Surrender Policy	Emotional campaigns, legal relief, growing participation	Weak reintegration, poor livelihood support
Narrative War	CAP initiatives, digital counter-propaganda	Urban Naxal influence, weak ideological contestation
Governance	Dashboard monitoring, KPIs, competitive rankings	Trust deficit, inconsistent implementation

e. Way Forward – Strategic Recommendations

- **Unified Intelligence Fusion**: Create dedicated Maoist intelligence grids at national and state levels for real-time sharing.
- **Hard–Soft Synchrony**: Align security force movements with welfare delivery—for example, DRG protection alongside PDS distribution.
- **Grassroots Development**: Prioritise tribal para-teachers, mobile health units, and micro-grids to build daily state presence.
- **Digital Counter-Ideology**: Invest in fact-checking platforms, regional-language storytelling, and credible counter-narratives.
- **Urban Ecosystem Monitoring**: Balance vigilance with safeguards—ensuring dissent is not criminalised, and UAPA use is judicially reviewed.

Conclusion

India's strategy against Left-Wing Extremism has moved from crisis management to consolidation. The hard data shows remarkable progress, yet strategic victory is not assured. As long as alienation persists, Maoist ideology will find space to survive.

Winning the jungle is not the same as winning the people. The real measure of success will be when tribals experience dignity, opportunity, and justice as lived realities, not slogans.

As one analyst observed: *"A war ends not when enemies surrender, but when hearts do."* To end the Maoist conflict permanently, India must wage not only a military campaign but also a moral one—rooted in governance, fairness, and hope.

The critical appraisal of India's counter-LWE strategy makes it evident that while security operations and developmental outreach have weakened the insurgency, the challenge of rehabilitation and reintegration remains unresolved. Surrendered cadres often find themselves in limbo—caught between state promises of support and social stigma, while facing threats from Maoist hardliners.

Without credible livelihood options and community acceptance, many risk slipping back into insurgency or drifting into other extremist networks.

Thus, the next crucial dimension in tackling Left-Wing Extremism is to assess rehabilitation models—their design, successes, and persistent challenges. This evaluation is vital to ensure that gains achieved through security and development are not undone by weak reintegration.

2.15 Rehabilitation Models and Challenges

a. Introduction

Rehabilitation of surrendered Maoist cadres has emerged as the decisive frontier of India's counter–Left-Wing Extremism (LWE) strategy. While security operations can dismantle insurgent bases and development schemes can win communities, enduring peace rests on whether those who once bore arms can be reintegrated into mainstream society with dignity, livelihood, and safety.

The idea is not merely to neutralise an adversary but to transform an individual into a citizen who becomes a partner in stability. Yet, despite the existence of central and state-level surrender and rehabilitation policies, implementation has remained uneven. Funding gaps, bureaucratic delays, social stigma, and security threats have often blunted the promise of these programmes, leaving many surrenderees in a precarious limbo.

b. Objectives of Rehabilitation

The goals of rehabilitation are both strategic and humanitarian, blending immediate counter-insurgency imperatives with long-term social stability:

- **Deradicalisation** – Helping former cadres move away from violent ideologies and embrace democratic participation.
- **Reintegration** – Enabling returnees to become part of the economic, social, and legal mainstream, rather than permanent outsiders.
- **Incentivisation** – Creating visible success stories so that active cadres are encouraged to surrender.
- **Disruption of Maoist Networks** – Weakening the chain of command by drawing away vulnerable foot soldiers.
- **Long-term Stability** – Preventing new recruitment by showcasing the state's compassion and credibility.
- **Intelligence Gathering** – Securing actionable insights on hideouts, financial channels, and recruitment pipelines through the cooperation of surrendered cadres.

c. Features of India's Rehabilitation Framework

India's rehabilitation framework operates through both national guidelines and state-level innovations. While broad principles are uniform, specific packages vary across affected states such as Chhattisgarh, Jharkhand, Odisha, and Maharashtra.

i. Monetary Incentives

The financial architecture is designed to provide immediate relief as well as medium-term sustenance:

- A one-time surrender grant, usually between ₹2.5 and ₹5 lakh, with higher amounts for senior commanders.
- A monthly stipend of ₹6,000 to ₹10,000, typically for a period of up to three years.
- Additional bonuses for the surrender of weapons—₹25,000 for small arms to ₹1 lakh for automatic weapons.

ii. Skill Training and Employment

Rehabilitation emphasises employability, aligning surrendered cadres with income-generating pathways:

- Short-term training in industrial training institutes (ITIs) in trades such as driving, tailoring, or welding.
- Linkages with livelihood schemes through self-help groups, MGNREGA, and MSME initiatives.
- Preferential recruitment into semi-formal roles such as Home Guards, Forest Guards, and civic contractual positions.

iii. Housing and Welfare Support

Housing and social security are integrated into the package to prevent relapse into insecurity:

- Allotments under Pradhan Mantri Awas Yojana (PMAY), both urban and rural, or state housing boards.
- Entitlement to ration cards, health insurance under Ayushman Bharat, and scholarships for children's education.

iv. Security Provisions

Safety nets are vital, especially in high-risk contexts where Maoist reprisals are common:

- Transit camps and safe houses located in neutral or urbanised areas.
- Escort arrangements for court visits and sensitive travel.
- Identity protection and discreet relocation where personal security is under serious threat.

d. Model Initiatives Worth Citing

A few state-level innovations stand out as successful experiments in shaping rehabilitation into a credible pathway:

State	Initiative	Outcome
Chhattisgarh	"Lone Varatu" campaign	Emotional framing and trust-building through community messaging led to over 400 surrenders.
Jharkhand	Surrender camps with NGO mediation	Built community trust, reduced recidivism, and encouraged family support in reintegration.
Odisha	Skill-linked rehabilitation in Malkangiri	Youth placed in local industries; schools reopened in villages once deserted by insurgency.

e. Challenges in Rehabilitation

Despite carefully designed policies, the reality of rehabilitation on the ground is far more uneven. What should serve as a gateway to peace often falters under fear, bureaucracy, and stigma.

i. Fear of Retaliation

Hardcore Maoist leaders often portray surrender as treason, branding defectors as traitors to the cause. Many returnees face threats of execution by underground networks, while others are subject to intimidation of their families.

In some cases, the absence of credible protection has forced surrendered cadres to reverse their decision—highlighting the fragility of state assurances.

ii. Patchy Delivery of Promised Benefits

The gap between policy and practice is stark:

- Delays in disbursing grants due to red tape erode trust.
- Skill programmes are often generic and mismatched with local labour markets.
- Follow-up monitoring is minimal, leaving surrenderees without guidance once the initial handholding ends.

In several districts, cadres continued to live in temporary shelters even two years after surrender, as housing allotments remained pending.

iii. Social Stigma and Identity Crisis

The challenge of social acceptance often outweighs material concerns.

- Ex-cadres are labelled as "traitors" or "agents of the police," especially in villages scarred by Maoist violence.
- Families face ostracism, while tensions within communities rise.
- The absence of psychological counselling deepens alienation, leading to depression and, in some cases, relapse into violence.

iv. Youthful Return to Violence

Young returnees are particularly vulnerable. With no sustainable livelihood or clear direction, they become easy targets for re-recruitment.

The lure of underground networks, coupled with exposure to extremist propaganda in urban digital spaces, increases the risk of recidivism.

v. One-Size-Fits-All Models

Uniform policy templates rarely account for the diverse experiences of surrenderees.

- Gender-specific trauma, child recruits, and disabled ex-combatants often remain invisible in mainstream rehabilitation plans.
- Without customisation, reintegration efforts struggle to address the complexity of individual needs.

f. Towards an Ideal Rehabilitation Model

To be effective, rehabilitation must be seen not as a transaction but as a transformation—from insurgent to citizen, from fear to dignity. The ideal model would rest on the following pillars:

- **Pre-Surrender Counselling** – Trusted mediators such as teachers, family members, or NGOs can act as bridges, encouraging cadres to consider reintegration.
- **Safe Passage Mechanisms** – Anonymous helplines and third-party intermediaries can ensure cadres cross over without fear of betrayal.
- **Personalised Reintegration Plans** – Skill mapping, tailored livelihood placement, and education pathways should replace generic programmes.
- **Social Rehabilitation** – Reintegration cannot succeed in isolation. Gram Sabha endorsement, community counselling, and cultural acceptance are essential.
- **Long-Term Monitoring** – Regular check-ins, grievance redressal systems, and peer support networks must ensure that surrenderees are not abandoned after initial benefits are exhausted.

As one field officer aptly observed: *"Rehabilitation is not a transaction. It is a transformation—from insurgent to citizen, from fear to dignity."*

Conclusion

Rehabilitation is not merely an exit route from armed rebellion; it is the bridge back to citizenship, justice, and hope. India's policies have evolved considerably, but their promise is often undermined by fear, stigma, and bureaucratic lethargy.

The Home Ministry's 2023 review revealed that only 35 percent of surrendered cadres in some districts had actually received all promised benefits—a sobering reminder of the trust deficit that endures.

As the cycle of Maoist violence recedes, the next frontier is not winning the war but securing the peace. Success will be measured not in surrenders counted, but in futures rebuilt. A surrendered youth should never look back—neither in regret for broken promises, nor in despair at neglect.

Justice V. R. Krishna Iyer once observed: *"You do not rehabilitate a person. You rehabilitate their hope."* Ensuring that hope endures is the true test of India's counter-LWE strategy.

The discussion on rehabilitation highlights that dismantling insurgency is not only about disarming cadres but also about reintegrating them into the moral and economic mainstream. Yet, rehabilitation is just one strand of the wider tapestry required to neutralise Left-Wing Extremism.

Countering an insurgency that is at once military, ideological, and socio-economic cannot rely on fragmented efforts. It demands a holistic, multi-dimensional framework that balances force with fairness, development with dignity, and state presence with community partnership.

This recognition has given rise to what can be described as the Five-Pillar Approach—a structured strategy that weaves together security, development, rights, perception management, and rehabilitation into one coherent design.

Moving from isolated interventions to an integrated doctrine, these five pillars represent the foundation upon which India's long-term victory over LWE must rest.

2.16 The Five-Pillar Approach to Counter Left-Wing Extremism

a. Introduction

India's campaign against Left-Wing Extremism (LWE) has gradually moved away from being understood as a purely military or policing problem. Experience has shown that the insurgency thrives not only on firepower but also on alienation, underdevelopment, and mistrust.

Out of this realisation has emerged a structured five-pillar approach, which combines the strength of kinetic action with the legitimacy of governance and the persuasiveness of narratives. This model offers a cohesive framework that balances constitutional values with security imperatives—aiming not simply to defeat rebels in battle but to dismantle the ecosystem of rebellion itself.

b. The Five Pillars Explained

At its core, the strategy rests on five interconnected foundations:

Pillar	Core Focus	Key Components
Security	Area dominance and tactical neutralisation	Special Forces (CoBRA, Greyhounds), CAPFs, surveillance tech, SAMADHAN doctrine
Development	Addressing structural causes of alienation	Roads (PMGSY), telecom (BharatNet), electricity (Saubhagya), Aspirational Districts

Pillar	Core Focus	Key Components
Rights-Based Governance	Restoring constitutional faith	Forest Rights Act, PESA Act, tribal representation, legal literacy
Rehabilitation	Reintegration of surrendered cadres	Monetary incentives, skill training, safe shelters, community reconciliation
Perception Management	Winning hearts and minds, countering propaganda	Civic Action Programmes, cultural outreach, counter-radicalisation messaging

c. Pillar-Wise Deep Dive

i. Security

Security forms the indispensable first layer, for without safety neither governance nor development can take root.

- Specialised jungle warfare units such as CoBRA, Greyhounds, and District Reserve Guards (DRG) bring terrain-specific expertise.
- Joint deployments of CAPFs and state police secure area dominance.
- Drones, UAVs, and GPS-enabled systems strengthen real-time surveillance.
- The unified command model, where district officers are evaluated against KPIs, enhances accountability.

In essence, security is the gate through which every other state initiative must pass.

ii. Development

Once security opens space, development fills it with opportunity, displacing insurgent influence.

- Roads, telecom towers, micro-grids, banks, schools, and hospitals now reach areas once dependent on Maoist parallel systems.
- Mobile ATMs and digital service centres extend financial inclusion.
- The Aspirational Districts Programme converges multi-sectoral improvements.
- Skill-building programmes and local industrial linkages provide livelihoods for tribal youth.

When ration cards, pensions, and electricity arrive before insurgent pamphlets, the promise of revolution begins to fade.

iii. Rights-Based Governance

True legitimacy is measured not only in service delivery but in empowerment.

- The Forest Rights Act (FRA) and Panchayats (Extension to Scheduled Areas) Act (PESA) restore dignity when implemented in spirit.
- Empowered Gram Sabhas and legal literacy campaigns reinforce faith in constitutional processes.
- Recruitment of tribals into the police, forest, and revenue departments fosters ownership of state institutions.

By ensuring rights and justice, governance directly undercuts Maoist narratives of exclusion.

iv. Rehabilitation

Rehabilitation converts former insurgents from liabilities into agents of stability.

- Monetary incentives and stipends provide sustenance.
- Vocational training and preferential employment create long-term pathways.
- Safe shelters and identity protection guard surrendered cadres from reprisals.
- In several states, public ceremonies symbolically normalise reintegration, transforming guerrillas into citizens.

By offering a dignified second life, rehabilitation shrinks the pool of alienated youth vulnerable to recruitment.

v. Perception Management

The final pillar lies in the battle of ideas.

- Civic Action Programmes (health camps, sports events, scholarships) bridge the state-community gap.
- Cultural festivals, folk arts, and local storytelling provide alternatives to Maoist propaganda.
- Digital platforms and social media campaigns counter misinformation.
- Civil society leaders, religious figures, and reformed insurgents act as credible messengers of peace.

Victory in the war of ideas, unlike battlefield gains, is enduring and transformative.

d. Why This Model Matters

The five-pillar framework represents the maturing of Indian statecraft in dealing with internal conflict. It acknowledges that brute force can kill rebels, but only justice and dignity can extinguish rebellion.

By weaving together security, development, governance, rehabilitation, and perception management, the strategy moves beyond containment to consolidation.

This holistic model disrupts recruitment pipelines, restores tribal trust, and reclaims the ideological space once monopolised by Maoists. It aligns counter-insurgency with constitutional morality, proving that a state which is trusted achieves more durable peace than a state which is merely feared.

Conclusion

The five-pillar approach reflects India's shift from reactive crisis management to strategic state-building. It is premised on the understanding that insurgency is not only about guns but also grievances. By integrating force with reform, technology with trust, and development with dignity, the model seeks not merely to suppress Left-Wing Extremism but to render it irrelevant.

As Kautilya's *Arthashastra* reminds us: *"A state that is feared may win battles. But a state that is trusted wins the war."*

The five-pillar framework illustrates how India has gradually transformed its fight against LWE into a balanced architecture of security, development, governance, rehabilitation, and perception management. It demonstrates that insurgencies rooted in socio-economic alienation can be contained when the state combines force with fairness and legitimacy.

Yet, the end of one struggle does not mean the end of internal security challenges. As the Maoist movement recedes, India faces a wider and more complex spectrum of threats—religiously motivated terrorism, global jihadist networks, homegrown radicalisation, cross-border sponsorship, and disruptive technologies such as drones and cyber warfare.

Unlike the geographically bounded conflict in the Red Corridor, these new threats are fluid, transnational, and digitally amplified.

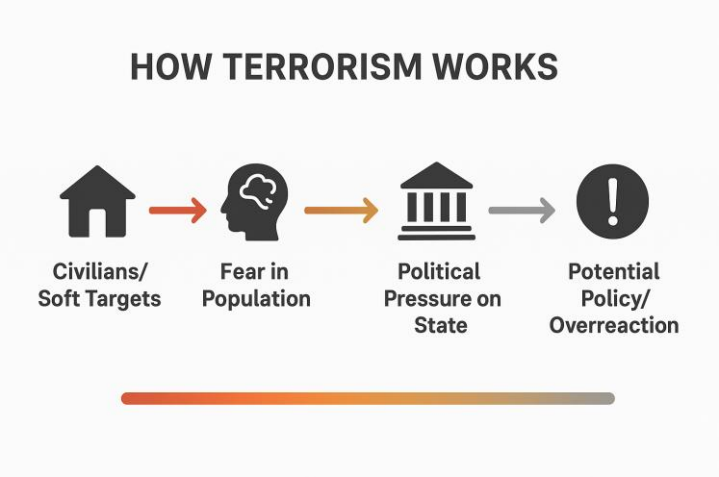
Thus, the conversation must now shift from insurgency in forests to terrorism in cities, from the ideology of class struggle to the ideologies of religious extremism, separatism, and digital radicalisation.

The next chapter explores how India engages with these evolving threats, examining their drivers, mechanisms, and the strategies required to counter them.

Chapter 3. Terrorism, Radicalisation & Emerging Threats

3.1 What is Terrorism?

Terrorism may be understood as the premeditated use of unlawful violence, particularly against civilians, with the intent of creating fear, coercing societies, or pressuring governments to concede to ideological, political, religious, or economic demands.



It represents a form of asymmetric warfare, where actors with limited conventional capacity—often non-state groups, sometimes state-sponsored proxies—use fear, spectacle, and selective brutality to undermine the authority of states with far greater military strength.

The United Nations High-Level Panel on Threats, Challenges, and Change (2004) offered a widely cited formulation:

"Any action intended to cause death or serious bodily harm to civilians or non-combatants, to intimidate a population, or to compel a government or an international organization to do or abstain from doing any act."

This definition highlights the twin essence of terrorism:

- Its violence is targeted not merely at individuals but at the psychology of societies.
- Its ultimate purpose is not destruction for its own sake but coercion through fear.

a. Distinguishing Terrorism from Related Concepts

Clarity requires that terrorism not be conflated with war, insurgency, or extremism, though these categories often intersect.

Concept	Description	Example
Terrorism	Use of violence to instill fear and achieve ideological goals through deliberate targeting of civilians.	2008 Mumbai attacks (26/11)
Insurgency	Armed rebellion against state authority, often with territorial or secessionist aims.	Naga insurgency in Northeast India
Extremism	Rigid, absolutist ideology that rejects pluralism and compromise; may remain non-violent.	Khalistani propaganda overseas
Radicalisation	Process by which individuals adopt extremist beliefs, which may eventually culminate in violence.	Online self-radicalisation of youth via ISIS propaganda

While insurgents may fight state forces directly and extremists may remain ideological, terrorism is distinct in its deliberate weaponisation of fear through civilian targets.

b. Core Characteristics of Terrorism

Terrorism is differentiated from ordinary criminal violence by a set of recurring features:

- **Political or Ideological Motive** – Every terrorist act pursues a larger cause (secession, religious enforcement, revolution, systemic destabilisation), distinguishing it from purely criminal objectives.
- **Deliberate Targeting of Civilians** – Markets, schools, places of worship, and transport hubs are chosen to maximise vulnerability and psychological shock.
- **Psychological Impact Beyond Physical Damage** – The true aim is to instill a climate of fear, magnifying insecurity across populations.
- **Asymmetric Tactics** – Small, mobile groups exploit surprise, stealth, and technology to challenge far larger state structures.
- **Spectacle and Media Amplification** – Attacks are choreographed for maximum visibility, ensuring virality in media and social platforms to serve propaganda ends.
- **Networked Organisation** – Contemporary terrorism is often decentralised, using dispersed cells, encrypted communication, and funding through hawala networks, cryptocurrency, and the dark web.

c. Strategic Objectives of Terrorist Groups

Though motives vary across regions and ideologies, terrorist organisations converge around recurring objectives:

- **Exerting Political Pressure** – Pakistan-backed groups in Jammu and Kashmir aim to internationalise the dispute through sustained violence.
- **Secessionist Agendas** – ULFA and NSCN seek to carve out independent homelands.
- **Religious Supremacy** – Transnational groups like ISIS pursue the establishment of a global Caliphate.
- **Eroding State Authority** – Maoists target police stations, convoys, and district HQs to symbolise state vulnerability.
- **Economic Disruption** – The 26/11 Mumbai attacks paralysed India's financial capital, undermining investor confidence.
- **Provoking State Overreaction** – High-profile attacks often aim to trigger communal backlash or excessive state repression, fuelling alienation and recruitment.

Conclusion

Terrorism must be recognised as a distinct phenomenon—separate from insurgency, extremism, or mere criminality. Its forms vary according to the motivations driving it, the methods employed, and the objectives sought.

From ethno-nationalist separatism to religious fundamentalism, from left-wing revolutionary movements to state-sponsored proxy warfare, each type of terrorism reveals a different facet of how violence is weaponised for political ends.

A careful classification of types of terrorism is not merely theoretical; it provides practical clarity for counter-terrorism strategy. The tools needed to counter a secessionist insurgent group differ significantly from those required to contain religious radicalisation or cyber-enabled lone-wolf attacks.

With this in mind, the next section explores the major types of terrorism, their distinctive features, and illustrative examples from both India and the global context.

3.2 Types of Terrorism

a. Introduction

Terrorism is not a uniform phenomenon. It manifests in diverse forms across ideological, geographical, and technological lines—each demanding a distinct counter-strategy. While some groups derive legitimacy from religious extremism, others weaponise political ideologies, ethnic grievances, or illicit economies such as narcotics trafficking.

In India's case, the challenge is compounded by porous borders, pluralistic social fabric, democratic safeguards, and a digitally open environment. These conditions allow terrorist organisations to constantly shift tactics—from guerrilla-style ambushes to grey-zone operations, hybrid warfare, and cyber-enabled radicalisation.

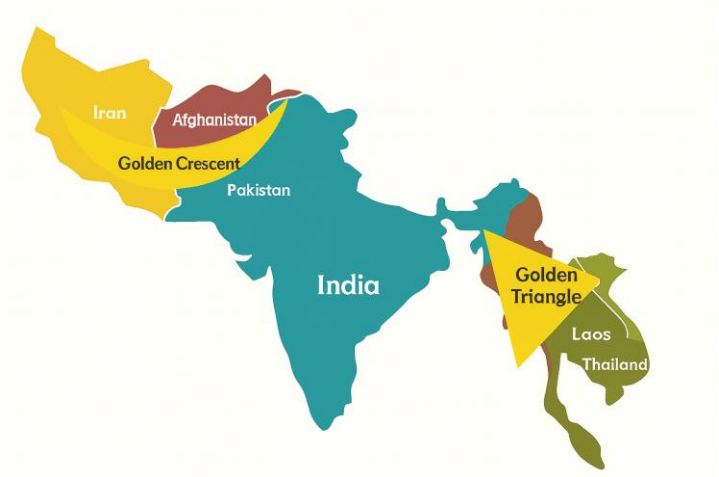
A nuanced classification of terrorism is therefore vital. It serves three key purposes:

- Formulating differentiated policies.
- Preventing misuse of anti-terror laws against legitimate dissent.
- Strengthening preventive intelligence frameworks.

As Clausewitz argued that war is the continuation of politics by other means, in the asymmetric age terrorism is the continuation of grievance by violent means, with its many forms acting as instruments of that larger struggle.

b. Classification of Terrorism

Terrorism in the modern world manifests in multiple forms, shaped by geography, ideology, religion, economics, and technology. Each type carries distinctive features, yet all share a common thread: the deliberate use of violence or coercion to destabilise societies and challenge state authority.



For India, which has endured decades of diverse terrorist threats, understanding these classifications is essential for designing appropriate counter-strategies.

i. Cross-Border Terrorism

This form originates from foreign soil, often aided by overt or covert state sponsorship. Pakistan has been the primary source, with groups such as Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM) infiltrating through the Line of Control (LoC).

Incidents: Mumbai attacks (2008), Pathankot airbase assault (2016), Pulwama bombing (2019).

Features: State sponsorship via Pakistan's ISI, LoC launchpads, narco-funding, diaspora-driven propaganda.

Counter-Strategy: Border fencing, advanced surveillance, calibrated military responses (e.g., Balakot airstrike), and international pressure through FATF and UN forums.

ii. Ideological Terrorism

Motivated by radical political or economic ideologies, this form seeks to overthrow constitutional governance. In India, Left-Wing Extremism led by the CPI (Maoist) exemplifies this threat.

Features: Class warfare narratives, IED use, ambushes on convoys, rural–tribal strongholds.

Counter-Strategy: The SAMADHAN doctrine blending force with development, backed by community mobilisation through schools, jobs, and infrastructure.

iii. Religious Terrorism

This variant justifies violence through extremist interpretations of religion.

- Islamist outfits: ISIS-K, Al-Qaeda in the Indian Subcontinent, Indian Mujahideen, SIMI.
- Khalistani separatists operating from abroad.

Features: Religious rhetoric, communal incitement, suicide bombings, safe havens abroad, diaspora mobilisation.

Counter-Strategy: Community engagement, deradicalisation in both physical and digital domains, and strict enforcement of laws such as UAPA.

iv. Cyber Terrorism

The rise of digital technologies has enabled terrorists to exploit cyberspace for propaganda, recruitment, disruption, and psychological warfare.

Examples: ISIS recruitment via Telegram, hacktivist attacks on Indian institutions, deepfake propaganda.

Features: Global reach, anonymity, cryptocurrencies, encrypted dark web forums.

Counter-Strategy: Strengthening CERT-In and NTRO, establishing cyber police stations, and empowering the Indian Cybercrime Coordination Centre (I4C).

v. Narco-Terrorism

This form links drug trafficking with terrorism, where narcotics proceeds fund extremist activity.

Examples: ISI–D-Company nexus exploiting Punjab; Golden Crescent and Golden Triangle drug flows fuelling insurgency in the Northeast and J&K.

Features: Terror financing through drug money, arms procurement, bribery of officials, social destabilisation via addiction.

Counter-Strategy: Coordination between NCB, ED, and state police, cross-border interdiction, and financial tracing under FEMA and PMLA.

vi. State-Sponsored Terrorism

Governments actively nurture or shelter terrorist groups to pursue strategic objectives under plausible deniability.

Examples: Pakistan's support to LeT and JeM; Chinese disinformation and cyber intrusions as new-age variants.

Features: Proxy violence, diplomatic friction, denial of accountability.

Counter-Strategy: Diplomatic isolation of sponsoring states, FATF and UN sanctions, and calibrated covert responses.

vii. Hybrid Warfare and Grey-Zone Terrorism

This form blends conventional force with irregular tactics, cyber tools, and perception warfare to weaken adversaries without open war.

Examples: Russia's tactics in Ukraine; China's "Three Warfares"—media, legal, psychological.

Features: Propaganda, lawfare, economic sabotage, cyberattacks, perception management.

Counter-Strategy: Integrated doctrines combining cyber defence, fact-checking units, and proactive cyber diplomacy.

Conclusion

India faces one of the world's most diverse spectrums of terrorism—from cross-border infiltrations to lone-wolf actors radicalised through social media. This multiplicity defies any one-size-fits-all solution.

It necessitates multi-tiered responses:

- Boots on the ground against guerrilla insurgents.
- Firewalls against digital extremists.
- Grassroots trust-building against ideological radicalisation.
- Strategic deterrence against state-sponsored proxies.

As NSA Ajit Doval cautions: *"Terrorism adapts faster than bureaucracy. Only intelligence, empathy, and adaptability can outpace it."*

The classification of terrorism demonstrates that violence today is not confined to bombs, bullets, or ambushes. Modern terrorist networks and hostile states increasingly employ non-kinetic tools—disinformation campaigns, cyber intrusions, narco-funding, lawfare, and psychological operations—that can destabilise societies just as effectively.

In the twenty-first century, the battlefield has expanded from jungles and borderlands to digital platforms, financial systems, and public perception. Understanding these non-kinetic dimensions of terrorism is critical, for they are harder to detect, harder to deter, and often more corrosive in the long run.

The next section will therefore explore these instruments of modern conflict, showing how they reshape terrorism into hybrid, multi-domain threats that demand equally adaptive responses.

3.3 Non-Kinetic Tools of Modern Terrorism and Warfare

a. Introduction

In the twenty-first century, terrorism has extended far beyond bombs and bullets. The battlefield has shifted from jungles and borderlands to courtrooms, digital platforms, financial systems, and the human mind.

Non-kinetic tools form the "silent arsenal" of modern terrorism and hybrid warfare—aimed not at destroying physical infrastructure alone but at destabilising societies, demoralising populations, discrediting governments, and distorting narratives.

These instruments exploit the very freedoms that define open democracies like India: freedom of speech, technological access, transparent legal systems, and pluralist discourse. From Maoist press releases portraying insurgents as defenders of tribal rights, to encrypted Telegram channels radicalising youth, to misuse of foreign funding regulations under the guise of human rights advocacy—the battlefield has become psychological, digital, legal, and symbolic.

As one analyst noted: *"The war is no longer about territory. It is for memory, perception, and legitimacy."* Understanding these arsenals is essential not merely for counter-terror operations but also for safeguarding the moral authority of the state in an age where disinformation spreads faster than bullets.

b. What are Non-Kinetic Tools?

Non-kinetic tools refer to methods that achieve political or strategic objectives without direct combat or explosives. They are designed to win minds, break willpower, and spread confusion—often without a single shot being fired.

In short:
"Winning without fighting, confusing without attacking, radicalising without touching."

c. Categories of Non-Kinetic Tools in Modern Terrorism and Hybrid Warfare

Tool Type	Core Objective	Key Tactics and Indian Examples
Psychological Warfare	Demoralise the public, erode trust in the state	Glorifying Maoist ambushes as "justice" for tribals; fake videos portraying Indian forces as brutal in J&K.
Lawfare (Legal Warfare)	Exploit judicial/legal systems to obstruct the state	PILs against anti-Naxal ops; misuse of RTI or human rights platforms to shield radical elements.
Information Warfare	Manipulate public opinion via propaganda/disinformation	Circulation of deepfakes, hate speech, fake news on WhatsApp & Telegram; Khalistani content on YouTube.
Cyber Tools	Enable anonymous networking, recruitment, planning	ISIS modules using dark web & crypto; hacking govt websites; attempts to infiltrate drones.
Financial & Narco Tools	Generate funds through illicit/shadow channels	Hawala via Dubai & PoK; misuse of foreign contributions by NGOs; narcotics smuggling via Punjab & Manipur.
Cultural & Identity Warfare	Undermine national unity via identity fault lines	Radical songs/posters glorifying Bhindranwale; anti-India cultural propaganda abroad.

Conclusion

Non-kinetic terrorism is a low-cost, high-impact strategy that requires neither armies nor explosives. Its strength lies in stealth: winning without fighting, destabilising without open confrontation, radicalising without physical contact.

For India, the challenge is heightened by three factors:

- An open digital ecosystem.
- A deeply plural society vulnerable to identity mobilisation.
- A legal framework grounded in liberty and due process rather than pre-emption.

As media theorist Marshall McLuhan presciently observed: *"Wars of the future will not be fought on land or sea, but in the minds of men."*

For India, this means evolving counter-terrorism beyond firepower—towards governance, resilience, and narrative control. From border control to browser control, and from reactive raids to pre-emptive civil-society resilience, the state must adapt to a conflict where perception often outweighs firepower.

The exploration of non-kinetic tools reveals how modern terrorism extends into psychological, digital, financial, and cultural domains. Yet, these methods do not operate in isolation—they are wielded by specific organisations with distinct ideologies, networks, and transnational linkages.

From Pakistan-backed outfits infiltrating across borders to homegrown radical networks exploiting local grievances, these groups represent the operational face of terrorism.

The next section therefore turns to an examination of the major terrorist groups—both domestic and foreign—that have shaped India's internal security environment and continue to pose evolving challenges.

3.4 Major Terrorist Groups: Domestic and Foreign

a. Introduction

India is among the few nations that confronts multi-dimensional terrorist threats simultaneously. These threats range from homegrown radical outfits to state-sponsored transnational groups, each with distinct ideologies, methods, and motivations. While some are rooted in Marxist revolutionary ideals, others pursue religious extremism, ethnic separatism, or digitally enabled radicalism.

Mapping these groups is not merely an academic exercise. It is essential for:

- Designing area-specific counter-insurgency strategies.
- Strengthening intelligence profiling.
- Anticipating the rise of networked terrorism, in which global jihadist ideologies are amplified by local cells and facilitated by narcotics and diaspora funding.

The overlap between domestic and foreign actors complicates the challenge further: international networks exploit India's internal cleavages, while indigenous cells act as enablers of transnational agendas.

b. Domestic Terrorist Groups

Group	Ideology / Objective	Active Areas	Key Threats
CPI (Maoist)	Maoist–Communist revolution through protracted armed struggle	Chhattisgarh, Jharkhand, Odisha, Maharashtra	Guerrilla ambushes, IEDs, disruption of governance
Students Islamic Movement of India (SIMI)	Islamist fundamentalism, aim of Islamic rule in India	Banned nationally; residual underground cells	Radicalisation, linkages with IM and global jihadi outfits
Indian Mujahideen (IM)	Urban Islamist terrorism; offshoot of SIMI	Delhi, UP, Karnataka, Maharashtra (now weakened)	Urban bombing campaigns (2007–13); sleeper cell activity
Khalistani Revivalist Cells	Sikh separatism, demand for Khalistan	Punjab; diaspora nodes in Canada, UK	Digital propaganda, arms smuggling, attempts at political infiltration

Group	Ideology / Objective	Active Areas	Key Threats
North-East Ethno-Terrorist Groups	Ethnic autonomy or secessionism	ULFA (Assam), NSCN (Nagaland), PLA (Manipur)	Attacks on security forces, extortion, safe havens in Myanmar & beyond

c. Foreign and Transnational Terrorist Groups Active Against India

Group	Base Country	Ideology / Goal	Operations Targeting India
Lashkar-e-Taiba (LeT)	Pakistan	Islamist jihad, Kashmir-centric	26/11 Mumbai attacks; recurrent LoC infiltrations
Jaish-e-Mohammed (JeM)	Pakistan	Islamist jihad, anti-India	Parliament attack (2001); Pulwama bombing (2019)
Hizbul Mujahideen	Pakistan, ISI-backed	Kashmiri separatism under Islamist banner	Recruitment in J&K; IEDs; targeted killings
Al-Qaeda in the Indian Subcontinent (AQIS)	Afghanistan–Pakistan region	Pan-Islamist caliphate vision, India focus	Propaganda modules; sleeper cells in Kerala & Bengal
Islamic State – Khorasan (IS-K)	Afghanistan (originating)	Global jihad; India labelled "Hind Province"	Online recruitment in Kerala & Telangana; multilingual propaganda
Tehreek-e-Taliban Pakistan (TTP)	Pak–Afghan border	Extremist Sunni Islamism	Indirect threat via Taliban–ISI–LeT nexus
Haqqani Network	Afghanistan–Pakistan	Proxy of Pakistan's ISI	Attacks on Indian assets in Afghanistan (Kabul embassy 2008, 2009)

d. Other Support Networks (Non-Direct Actors)

- **D-Company (Dawood Ibrahim network):** Financial and logistical hub for narco-terrorism, extortion, and arms smuggling on behalf of LeT and ISI.
- **Sikhs for Justice (SFJ):** Diaspora-based organisation (US, Canada) promoting Khalistani propaganda and legal warfare against India.
- **Pakistan's ISI:** Central enabler—providing training, arms, shelter, and funding to multiple groups.
- **Radical diaspora networks:** Streamline funding and spread propaganda through social media campaigns, fundraisers, and "rights-based" advocacy.

Conclusion

India's counter-terrorism challenge lies not merely in neutralising groups militarily but in disrupting the ecosystems that sustain them—their financial arteries, ideological sanctuaries, and digital platforms. Today, the battlefield is as much in encrypted chatrooms and diaspora networks as in forest hideouts and border infiltration routes.

As NSA Ajit Doval reminds: *"You cannot fight 21st-century terrorists with 20th-century tools."* India's strategy must therefore be multi-layered—confronting kinetic threats, countering ideological warfare, and hardening digital and financial frontiers simultaneously.

The mapping of terrorist organisations underscores the diversity of threats—from Maoist insurgents in forest belts to Islamist proxies across the border, from North-East secessionists to diaspora-driven Khalistani propaganda.

Yet, beyond their names and geographies, what truly matters is the pattern of their behaviour:

- How these groups recruit, sustain, and adapt.
- Why some groups fragment while others regenerate.
- How alliances form across ideological divides.
- How digital ecosystems allow even weakened outfits to retain influence.

It is this dynamic of behaviour—rather than static labels—that determines the resilience of terrorist networks and the effectiveness of counter-strategies. For India, understanding these behavioural patterns is critical.

The next section will therefore distil the key observations on terrorist group dynamics in India, highlighting the structural and strategic trends that shape their persistence and evolution.

3.5 Key Observations on Terrorist Group Dynamics in India

a. Introduction

Terrorism in India today is no longer bounded by region, ideology, or geography. It has transformed into a networked, transnational, and tech-enabled ecosystem, where the lines between insurgency, diaspora politics, propaganda, and digital extremism are increasingly blurred.

This evolution demands a multi-domain response strategy that cannot rely solely on conventional kinetic operations but must also anticipate overlapping threats across cyberspace, civil society, and financial systems.

i. Convergence of Threats: Operational and Ideological Fusion

Insurgent groups are increasingly transcending original boundaries of identity and ideology.

- Maoist networks in central India have exchanged logistical know-how with Northeast insurgents.
- So-called urban Naxal cells echo themes of victimhood and repression that mirror radical Islamist propaganda.
- In digital spaces, separatist rhetoric, communal incitement, and anti-state narratives fuse into a shared grievance ecosystem.

This convergence makes classification less relevant than capability, as disparate networks coalesce around hostility to the Indian state.

ii. State Sponsorship as Strategic Backbone

The backbone of terrorism against India remains state sponsorship—particularly from Pakistan.

- Pakistan's ISI provides safe havens, training, arms, and guidance to LeT, JeM, and Hizbul Mujahideen.

- Indian dossiers repeatedly trace financial flows and handlers back to Pakistan's deep state.
- Islamabad continues its doctrine of "strategic depth", treating terrorism as a cost-effective foreign policy tool.

The fusion of state resources with non-state actors remains one of India's most intractable challenges.

iii. Diaspora-Driven Radicalisation and Funding

Diaspora groups have emerged as amplifiers of extremist agendas, leveraging the freedoms of Western democracies.

- Sikhs for Justice (SFJ) campaigns such as *Referendum 2020* promote Khalistani separatism from Canada, UK, and US.
- Diaspora activism provides visibility, legitimacy, and funding pipelines through remittances, cryptocurrencies, and front NGOs.
- These networks weaponise legal activism and global narrative influence.

The diaspora thus acts as a triple force: financier, advocate, and propagandist.

iv. Digital Expansion of Terrorism

The digital domain has reshaped recruitment, training, and propaganda.

- Training camps are replaced by encrypted Telegram channels and dark web forums.
- Propaganda takes the form of memes, deepfakes, and viral hate campaigns.
- Lone-wolf actors self-radicalise via YouTube, Instagram, or WhatsApp.

In many ways, terrorism now functions like a start-up: decentralised, agile, and invisible until activation.

v. Cycles of Dormancy and Revival

Terrorist groups in India rarely disappear—they mutate, rebrand, or lie dormant before reviving.

- SIMI and its offshoot Indian Mujahideen resurface in altered forms.
- The Khalistan movement, assumed dormant post-1990s, has been digitally revived via diaspora activism.
- ISIS-K modules have appeared in Kerala, Telangana, and J&K.

These cycles highlight the peril of complacency: decline often masks incubation and regeneration.

vi. Blurring of Region-Specific Threat Maps

Traditional geographical associations of terrorism are collapsing.

- Kashmir is no longer the sole theatre of Islamist militancy.
- Maoist strategies echo in urban intellectual activism.
- Radicalisation reaches youth in Kerala and Bengal through transnational content.
- NGOs in Delhi may inadvertently channel funds into Maoist or Islamist networks.

Terrorism today is less about territorial strongholds and more about ideological contagion and digital reach.

Conclusion

India's terror landscape has mutated into fluid, converging ecosystems, where Maoist ambush tactics, Islamist digital radicalisation, and diaspora-funded separatism reinforce one another. The challenge lies not only in neutralising visible threats but in anticipating concealed and adaptive forms.

As General Bipin Rawat observed: *"In the age of hybrid threats, the enemy may not wear a uniform, carry a flag, or even live within your borders."*

India must therefore build resilience across cyberspace, civil society, financial systems, and international diplomacy to stay ahead of shifting dynamics.

The analysis of group dynamics shows that modern terrorism persists not merely through arms and ideology but through its ability to regenerate via radicalisation and recruitment.

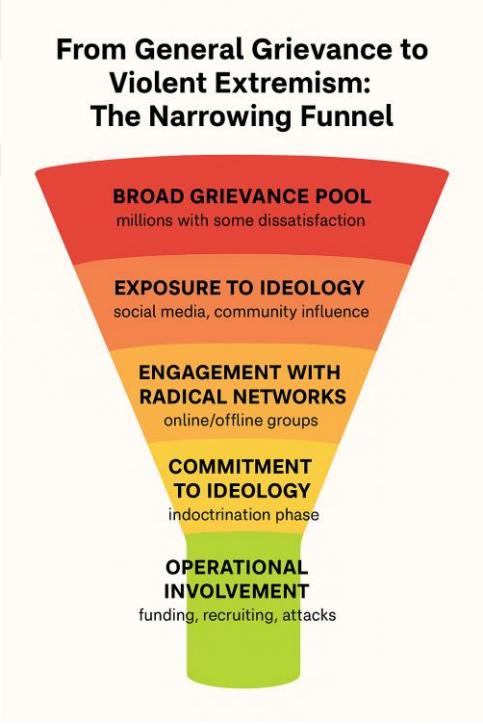
Whether through Maoist underground cells, Khalistani diaspora propaganda, or ISIS-inspired online networks, the lifeblood of terrorism lies in creating new cadres, sympathisers, and digital followers.

The next section will therefore examine radicalisation and recruitment pipelines, tracing the stages, methods, and vulnerabilities through which ordinary individuals are transformed into operatives of extremist causes.

3.6 Radicalisation and Recruitment Pipelines

a. What is Radicalisation?

Radicalisation may be defined as the gradual process through which an individual or group adopts extreme views that reject democratic norms, pluralism, and the legitimacy of the existing socio-political order. This process often culminates in the justification, support, or use of violence to achieve ideological goals.



Unlike dissent or political activism, which operate within democratic frameworks, radicalisation represents a departure into absolutist worldviews. It is characterised by:

- Binary thinking framed as "us versus them."
- Deep disillusionment with mainstream institutions.
- Moral justifications for violence against the state or targeted communities.

Radicalisation may occur:

- Offline – through clerics, peer groups, family, or local mentors.
- Online – via social media platforms, encrypted chat apps, gaming networks, or dark web forums.

The digital revolution has accelerated and globalised radicalisation, bypassing traditional surveillance and allowing extremist ideologies to travel across borders instantly.

As one counter-radicalisation strategy notes:
"Terrorism is the action. Radicalisation is the transformation that precedes it."

b. Stages of Radicalisation: A Simplified Four-Step Model

Radicalisation typically unfolds in progressive stages, though individuals may move through them at different speeds—or skip stages entirely in cases of "flash radicalisation."

Stage	Explanation	Common Indicators
Pre-Radicalisation	Ordinary life stage, but marked by underlying feelings of alienation or grievance.	Identity crisis, discrimination, personal loss, social isolation.
Self-Identification	Initial exploration of extremist ideologies; violence seen as a possible solution.	Sudden religiosity, withdrawal from peers, distrust in institutions.
Indoctrination	Deepening belief through repeated exposure, peer influence, or mentoring.	Encrypted group chats, echo chambers, ideological rigidity.
Jihadisation / Action Phase	Commitment to act, either through recruitment, funding, or direct violence.	Travel attempts to conflict zones, efforts to procure weapons, readiness for attacks.

In the digital era, *"flash radicalisation"* has become common—where individuals leap directly from curiosity to violent intent within weeks rather than years.

c. Drivers of Radicalisation in India and Globally

Radicalisation is rarely mono-causal. It emerges from a complex interplay of personal psychology, socio-economic conditions, governance failures, religious or cultural narratives, and digital ecosystems. Understanding the "why" is more critical than the "who" or "how."

i. Psychological Drivers

At the individual level, radicalisation is often rooted in unmet emotional and cognitive needs.

- **Identity Crisis** – Feelings of not belonging—whether to family, community, or nation—create openings for extremist ideologies. Urban Muslim youth in India and Europe drawn to the Islamic State exemplify this.
- **Search for Meaning** – Alienated or traumatised youth are attracted to movements offering a "higher calling." Recruits from Kerala and Tamil Nadu were lured into ISIS by narratives of divine mission.
- **Revenge and Grievance** – Personal or collective losses often fuel anger. Families of encounter victims in central India have joined Maoist ranks.
- **Cognitive Closure** – Extremist ideologies thrive on rigid, black-and-white thinking. Maoist cadres routinely dismiss democratic politics as "bourgeois compromise."

ii. Socio-Economic Drivers

Economic deprivation and social exclusion create fertile ground for extremist narratives.

- **Poverty and Unemployment** – Lack of livelihoods makes tribal youth in Bastar and Dantewada vulnerable to Maoist recruitment.
- **Illiteracy and Misinformation** – Limited education weakens resilience against propaganda, as seen in youth swayed by distorted sermons.
- **Social Exclusion** – Caste and tribal oppression deepen resentment, mobilised by extremist recruiters.
- **Urban Marginalisation** – Ghettos and segregated settlements foster alienation. Muslim enclaves in Uttar Pradesh or Assam have occasionally become breeding grounds for radical influence.

iii. Political and Governance Drivers

Failures of governance and perceptions of injustice often act as catalysts.

- **State Excesses** – Allegations of custodial abuse or heavy-handed policing fuel extremist propaganda. J&K unrest post-2010 and Maoist exploitation of *Salwa Judum* excesses are examples.
- **Weak Local Governance** – Governance vacuums allow radicals to establish parallel systems like Maoist *Jan Adalats* or Taliban-style courts.
- **Delayed Justice** – Prolonged trials entrench grievances, contributing to Sikh radicalisation post-1984 or narratives after the Godhra riots.
- **Selective Enforcement** – Perceptions of discriminatory laws (e.g., CAA protests) are reframed by extremist groups to mobilise dissent.

iv. Religious and Cultural Drivers

Religion and culture, when misappropriated, become potent instruments of mobilisation.

- **Scriptural Misinterpretation** – ISIS selectively quotes scripture to justify violence.
- **Charismatic Preachers** – Influential figures such as Zakir Naik or digital sermonisers emotionally sway audiences.
- **Historical Grievances** – Operation Bluestar and the 1984 riots are invoked by Khalistani groups to sustain militancy.
- **Perceived Cultural Erosion** – Narratives of cultural loss feed extremism, including Hindutva-driven conspiracy theories such as "love jihad."

v. Digital Ecosystem Drivers

The digital age has accelerated, anonymised, and amplified radicalisation.

- **Echo Chambers** – Algorithms push individuals from mainstream content into extremist material e.g., YouTube rabbit holes.
- **Encrypted Messaging** – Platforms like Telegram provide secure spaces for indoctrination.
- **Gamification of Jihad** – Groups like IS-K present violence as "achievement levels," appealing to young recruits.
- **Viral Deepfakes** – Fabricated atrocity videos circulated in Kashmir fuel anger and mobilisation.

vi. Diaspora and Transnational Drivers

Overseas networks and global politics increasingly shape radicalisation in India.

- **Diaspora Echo Chambers** – Organisations such as *Sikhs for Justice* amplify Khalistani narratives from Canada and the UK.
- **Foreign Funding and NGOs** – Misuse of FCRA funds has supported pro-Maoist literature and campaigns.
- **Global Geopolitics** – Conflicts like Palestine or Iraq are invoked by Indian ISIS recruits as justifications for joining global jihad.

Conclusion

Radicalisation is not a sudden leap into violence but a gradual erosion of critical thinking, empathy, and belonging. Its roots lie less in ideology itself and more in unresolved grievance, fractured identity, and persuasive propaganda.

In the digital age, a single WhatsApp forward can achieve in hours what once required months of indoctrination. Countering radicalisation therefore demands more than policing—it requires prevention, digital literacy, community resilience, and meaningful reintegration of at-risk youth.

As the UK's *Prevent Strategy* reminds us: *"You cannot bomb an ideology into silence. You must outthink it, out-narrate it, and out-include those drawn to it."*

The study of radicalisation and recruitment pipelines reveals how individuals move from grievance to indoctrination, and in some cases to violent action. At the heart of this transformation lies the digital ecosystem, the most powerful accelerator of modern extremism.

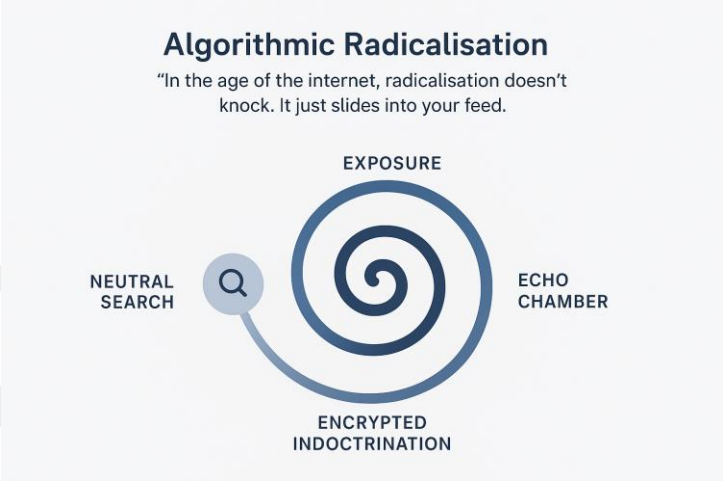
Unlike traditional radicalisation, which relied on clerics or recruiters, today's processes are shaped by online platforms that globalise grievances, personalise propaganda, and anonymise extremist networking.

The next section therefore examines online radicalisation in depth—its methods, platforms, and challenges—highlighting why cyberspace has become the new frontline of terrorism.

3.7 Online Radicalisation: The "Silent Enabler"

a. What is Online Radicalisation?

Online radicalisation refers to the process by which individuals—often isolated, disillusioned, or vulnerable—are exposed to extremist ideologies through digital platforms. This exposure pushes them to adopt radical worldviews, and in some cases, to translate belief into violent action. Crucially, this occurs without any direct physical contact with recruiters or training camps.



Its danger lies in its nature: anonymous, borderless, unregulated, and fast-moving. Online radicalisation has become one of the most potent vectors of twenty-first century terrorism.

b. Why is it Called a "Silent Enabler"?

Online radicalisation is termed a silent enabler because it magnifies extremism without triggering early warning signals.

- **Invisible** – Unfolds in private chatrooms, encrypted groups, or comment threads beyond the reach of policing.
- **Individualised** – Lone users can shift from curiosity to violent commitment without attending a mosque, camp, or rally.
- **Scalable** – A two-minute viral video or meme can influence thousands across continents instantly.
- **Deniable** – Terror groups can distance themselves from lone actors, preserving plausible deniability.

c. Mechanisms of Online Radicalisation: The Indian Context

In the digital age, entire pathways into extremism can unfold through a smartphone, often without an individual ever meeting a handler. For India—where hundreds of millions are first-generation internet users—this poses an acute challenge.

i. Algorithmic Echo Chambers

- Platforms like YouTube, Instagram, and Facebook push users toward more provocative content to maximise engagement.
- A casual search for religious lectures can escalate into exposure to jihadist sermons or separatist propaganda.

Indian Examples: Online jihadist lectures, Instagram reels glorifying martyrdom, curated playlists normalising violence as religious duty.

ii. Enclosed Encrypted Ecosystems

- Apps like Telegram, Threema, and Element create secure sanctuaries for indoctrination.
- Content includes indoctrination manuals, bomb-making guides, and extremist magazines (*Dabiq, Voice of Hind*).

Indian Examples: Kerala youth joining IS-K via Telegram; Maoist collectives sharing tactical material in encrypted groups.

iii. Gamification and Visual Warfare

- Extremists borrow gaming aesthetics, turning violence into adventure and martyrdom into "levels" of achievement.
- Memes, animations, and digital posters simulate rewards familiar to online gamers.

Indian Examples: Jihadi cartoons in gamer style; Khalistani posters mimicking first-person shooter games.

iv. Anonymised Financing

- Cryptocurrencies and dark web wallets enable untraceable micro-payments.
- Fake digital identities help purchase SIM cards and online services for covert operations.

Indian Examples: Tamil Nadu youth receiving IS-linked crypto transfers; SIMs procured through forged digital KYC.

v. Narrative Hijacking

- Extremist actors hijack legitimate grievances, reframing them as oppression narratives.
- Fake news, edited clips, or deepfakes cast the state as an oppressor and militants as liberators.

Indian Examples: Encounter killings reframed as "martyrdom"; fabricated atrocity videos circulated in Kashmir; selective amplification of Palestine to mobilise Indian sympathisers.

d. Why It is Hard to Detect

- **No physical links** – Self-radicalised actors operate without command chains.
- **Anonymity tools** – VPNs, burner phones, and temporary IDs mask activity.
- **Rapid timelines** – Radicalisation can occur in weeks rather than years.
- **Camouflaged content** – Propaganda disguised as sermons, lectures, or protest art.
- **Jurisdictional hurdles** – Foreign-hosted servers and lenient regimes delay responses.

e. Indian Case Studies

- **Kasargod IS Module (Kerala):** 21 youths radicalised via Telegram & YouTube, later travelled to Afghanistan to join IS.

- **Khalistani Digital Content (Punjab):** Songs & posters glorifying Bhindranwale, amplified by diaspora networks in Canada.
- **IS Hyderabad Module:** Youth radicalised through online sermons & extremist magazines; arrested while plotting attacks.
- **Urban Maoist Recruitment:** Students influenced by digital pamphlets & online campaigns framing "Dalit resistance."

Conclusion

Online radicalisation is no longer fringe; it is mainstream, mobile, and multiplying. With only a grievance and a smartphone, a youth can be transformed into an extremist without crossing borders or meeting handlers.

As one analyst remarked: *"In the age of the internet, radicalisation doesn't knock. It just slides into your feed."*

The exploration of online radicalisation shows how algorithms, encrypted spaces, and digital propaganda now drive extremism silently yet powerfully.

But if radicalisation is the disease, the natural question becomes: *what is the cure?* Security crackdowns alone cannot dismantle belief systems or prevent vulnerable individuals from slipping into extremist echo chambers.

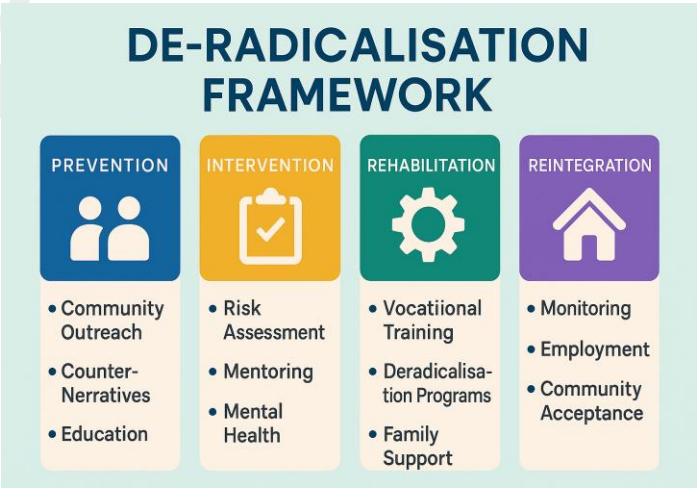
What is required is a comprehensive architecture of counter-radicalisation—combining policies, digital monitoring, deradicalisation counselling, and community-based resilience.

The next section therefore surveys counter-radicalisation measures in India and abroad, drawing lessons, highlighting gaps, and identifying best practices to build societies that are not just secure, but also resistant to extremist ideologies.

3.8 Counter-Radicalisation Measures (Indian and Global)

a. Introduction

In today's polarised and digitally connected world, radicalisation is neither distant nor gradual. It is increasingly local, viral, and invisible—spreading through WhatsApp forwards, encrypted Telegram groups, urban campuses, and even remote tribal belts. This makes counter-radicalisation one of the most critical frontiers of internal security.



Unlike de-radicalisation, which focuses on rehabilitating those already drawn into extremist ideologies, counter-radicalisation is preventive and strategic. It seeks to neutralise the root causes—psychological, social, political, economic, or religious—that make individuals vulnerable in the first place.

Effective counter-radicalisation therefore requires a whole-of-society approach:

- Families and schools act as early warning systems.
- Religious leaders and influencers serve as correctors of extremist narratives.
- Technology and intelligence agencies monitor digital ecosystems.
- The state's legitimacy provides the long-term immune system against extremist ideologies.

As one practitioner aptly put it: *"Radicalisation begins in the mind. Counter-radicalisation must begin in society."*

b. Why Counter-Radicalisation is Crucial

- De-radicalisation pulls back individuals already caught in extremist ideologies.
- Counter-radicalisation prevents vulnerable groups from entering the pipeline at all.

This makes it pre-emptive, holistic, and community-centred—involving not just law enforcement but also educators, faith leaders, civil society, and digital platforms.

c. Counter-Radicalisation Measures: Indian and Global Practices

i. Community Engagement

Grassroots outreach remains the first line of defence. Local actors often enjoy more credibility than state agencies.

Indian Examples:

- Village outreach in Jammu & Kashmir, designed to reduce alienation.
- *Mohalla* committees in Uttar Pradesh, which mediate during communal tensions.
- Imam-led counselling sessions, clarifying extremist misinterpretations of faith.

ii. Counter-Narrative Campaigns

Extremist propaganda thrives when unchallenged. Counter-narratives must not only refute extremist claims but also provide positive visions of belonging, dignity, and opportunity.

Indian Examples:

- Police-run YouTube channels that showcase stories of youth empowerment.
- Cultural festivals in Maoist-affected areas, restoring faith in state presence.
- Podcasts in Kashmir, highlighting inclusive traditions of Sufi Islam.

iii. Legal and Pre-Emptive Tools

Legislation gives the state authority to disrupt extremist activity before mobilisation turns violent.

Indian Examples:

- **Unlawful Activities (Prevention) Act (UAPA):** Designates individuals and organisations as terrorists.
- **National Investigation Agency (NIA) Act:** Provides centralised counter-terror investigations.
- **Information Technology Act, Section 69A:** Enables blocking of extremist websites.
- Regular takedowns of radical Telegram and WhatsApp groups spreading propaganda.

iv. Rehabilitation and De-Radicalisation Models

Preventive approaches also demand exit pathways for individuals drifting toward extremism. Not all recruits are hardened; many can be redirected through counselling, education, and vocational training.

Indian Examples:

- Kerala's counselling initiatives for vulnerable youth exposed to extremist sermons.
- Rehabilitation schemes in Manipur offering jobs and stipends to surrendered militants.
- Education- and employment-linked programmes for at-risk youth in Jammu & Kashmir.

v. Digital Surveillance and Cyber Tracking

With online platforms as the primary radicalisation arena, digital monitoring is indispensable.

Indian Examples:

- **Indian Cyber Crime Coordination Centre (I4C):** Tracks online radical content and funding pipelines.
- **National Technical Research Organisation (NTRO):** Cyber intelligence against extremist communication networks.
- Home Ministry–run cyber cells mapping surface web, deep web, and encrypted platforms.

d. Global Counter-Radicalisation Models and Best Practices

Country / Initiative	Key Features	Lessons for India
Saudi Arabia – PRAC (Prevention, Rehabilitation, Aftercare)	Combines religious re-education with family counselling and post-release aftercare.	Value of culturally rooted religious correction.
United Kingdom – Channel (PREVENT)	Early identification in schools/workplaces; avoids criminalisation stigma.	Importance of community-led prevention over state coercion.
Indonesia – Soft Deradicalisation	Engages former extremists as counsellors; counters ideology with moderate clerics.	Demonstrates peer credibility and narrative correction.
Singapore – Religious Rehabilitation Group (RRG)	Islamic scholars debunk jihadist interpretations in prisons, while families are included.	Shows effectiveness of theological correction + family support.
Denmark – Aarhus Model	Offers mentoring, job placement, housing, and community partnerships.	Proves the power of welfare-driven reintegration.

Counter-radicalisation is not just a security imperative—it is a societal resilience project. In India, where democracy, diversity, and digital openness coexist with vulnerabilities, the challenge is uniquely complex.

Global practices—from Saudi Arabia's religious re-education to Denmark's welfare-driven Aarhus Model—show that success comes when states balance security with empathy, law with legitimacy, and enforcement with inclusion.

As one counter-radicalisation maxim reminds us:
"You cannot bomb an ideology into silence. You must out-narrate it, out-think it, and out-include those vulnerable to it."

e. Key Pillars of an Effective Counter-Radicalisation Strategy

Radicalisation thrives in the shadows of grievance, alienation, and mistrust. Countering it therefore requires more than surveillance or enforcement; it calls for a comprehensive framework that builds trust, resilience, and social belonging. Five interlinked pillars form the foundation of an effective counter-radicalisation strategy.

i. Community-Centric Approach

Countering radicalisation cannot be left to the state alone. Families, educators, clerics, and youth mentors are often the first to notice behavioural shifts in vulnerable individuals, and their role is indispensable in prevention.

How it works: Religious leaders, teachers, and parents can serve as early detectors and correctors. Non-policing spaces—such as *mohalla* committees or youth clubs—provide dialogue platforms that foster belonging. Interfaith initiatives help debunk exclusivist ideologies and reinforce pluralism.

Indian Examples:

- Jammu and Kashmir's Village Engagement Programme, where police and clerics jointly address youth concerns.
- *Mohalla* peace committees in Uttar Pradesh, which have successfully diffused communal flashpoints.

"Those closest to the vulnerable are best placed to intervene—before radicalisation takes root."

ii. Psychological and Social Support Systems

Radicalisation is rarely the product of ideology alone; it often grows out of unhealed trauma, alienation, or identity crises. Addressing these personal wounds is central to long-term prevention.

How it works: Trauma counselling, mental health support, and grievance-redressal spaces can prevent individuals from seeking solace in extremism. Involving former radicals in rehabilitation lends authenticity to counter-narratives, showing that change is possible.

Indian Example: Kerala's de-radicalisation initiative, which blends psychological counselling, family involvement, and vocational training for vulnerable youth.

"If the wound is personal, the healing too must be personal."

iii. Technology-Enabled Vigilance

As recruitment increasingly shifts online, vigilance in the digital domain is indispensable. Extremist actors thrive in anonymity, often concealed within encrypted ecosystems.

How it works: Monitoring encrypted apps, dark web forums, and social media platforms enables early disruption. Collaboration with global tech firms such as YouTube, Telegram, and X (Twitter) ensures rapid takedown of harmful content. AI and machine learning tools can detect suspicious behavioural patterns in real time.

Indian Examples:

- Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs.
- Cyber Volunteers Programme, which allows citizens to anonymously report radical content.

"Today's jihadist may not wear a uniform—but he surely has a username."

iv. Narrative-Based Counter Strategies

Extremist propaganda thrives on powerful stories of grievance, martyrdom, and injustice. The antidote lies not merely in suppressing such narratives, but in offering compelling alternatives rooted in hope, belonging, and purpose.

How it works: Positive role models, patriotic accounts, and interfaith collaboration must be amplified. Youth-driven cultural platforms—music, art, theatre, podcasts—help reclaim spaces online and offline. Former radicals, influencers, and artists can serve as credible messengers with authenticity.

Indian Examples:

- "We The People" campaigns.
- Local music festivals in Maoist-affected regions.
- Madrassa lectures delivered by moderate clerics.

"If propaganda is poetry, counter-narrative must be prose—with power and purpose."

v. Human Rights–Respecting Law Enforcement

Over-securitised responses can inadvertently deepen alienation, pushing undecided individuals toward extremist camps. The state's legitimacy depends on being firm against violence yet scrupulously fair in methods.

How it works: Avoiding blanket profiling on religion, caste, or region is critical. Due process, speedy trials, and transparent investigations build trust in justice. Police training in negotiation, cultural sensitivity, and community engagement ensures firmness without repression.

Indian Example: Jammu and Kashmir Police's *Operation Milo Naap*, which prioritised surrender and counselling over indiscriminate arrests—balancing firmness with fairness.

"State legitimacy is the strongest antidote to radical ideology. Justice must not only be done—it must be seen to be done."

Conclusion

Radicalisation is not defeated by force alone. It is overcome when vulnerable individuals find belonging before they find a cause to hate. The essence of counter-radicalisation lies at the intersection of justice, dignity, opportunity, and prevention—where communities act as co-guardians of peace and the state is viewed as a partner, not a predator.

As terrorism expert Rohan Gunaratna reminds us: *"The best counter-terror strategy is a well-functioning democracy."*

Counter-radicalisation measures highlight that the battle against extremism is as much about narratives, communities, and trust as it is about force. Yet, while societies refine preventive frameworks, terrorist organisations are innovating constantly—adopting new tools in technology, finance, and culture to stay ahead of state responses.

From drones and cryptocurrencies to encrypted propaganda channels and narco-networks, the instruments of modern terrorism now extend far beyond the gun and the bomb. The next section therefore explores this contemporary toolkit of terrorism, examining the evolving methods, technologies, and tactics that define today's threat landscape.

3.9 Tools and Trends in Modern Terrorism

a. Introduction

Modern terrorism has undergone a profound transformation. The contemporary terrorist is no longer confined to jungles or battlefields; he operates equally in the cloud, on encrypted apps, and within narratives that manipulate identity and grievance. Guns and grenades are still used, but cyberspace, social media, drones, cryptocurrencies, and even democratic institutions have become the new theatres of conflict.

The rise of lone wolves, deepfakes, and algorithm-driven propaganda has made terrorism more anonymous, agile, and asymmetrical than ever before. Groups now invest as much in perception-building as in armed action, aiming to destabilise democracies and weaponise trust itself.

In this era, understanding the tools and trends of terrorism is as vital as tracking the actors themselves. This section maps how terrorism now spans the physical, digital, psychological, and legal domains, and how India must adapt to counter these hybrid threats.

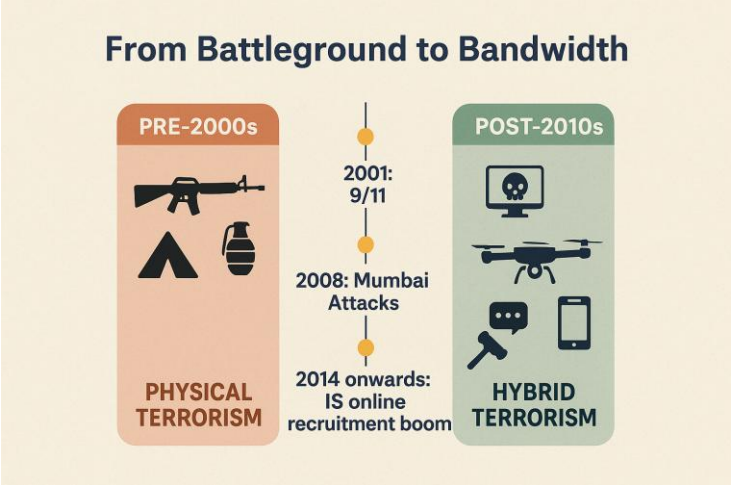
"The new terrorist is not just a bomber—he is a broadcaster, a hacker, and a storyteller."
— Adapted from Bruce Hoffman

b. Tools Used by Modern Terrorists

i. Cyber Tools

Terrorists and hostile actors employ hacking not only to steal sensitive data but also to compromise critical infrastructure. Disrupting power grids, defence communication networks, or financial platforms can paralyse a state without firing a shot.

Indian Example: Attempted hacks on Ladakh's power grid, reportedly linked to Chinese cyber groups, and fake defence recruitment portals used to phish sensitive information from youth.



ii. Encrypted Communication Platforms

End-to-end encryption provides extremists with secure channels for planning, propaganda, and recruitment. Manuals, indoctrination literature, and operational blueprints are circulated in closed groups, making conventional surveillance ineffective.

Indian Example: The Islamic State module in Kerala relied on encrypted Telegram channels to coordinate and distribute radical material while evading monitoring.

iii. Deep Web and Cryptocurrency

The dark web has emerged as a marketplace for weapons, forged documents, and SIM cards, while cryptocurrencies enable anonymous, borderless funding. Together, they form a financial and logistical backbone for clandestine operations.

Indian Example: Cryptocurrency transfers uncovered by the NIA linking Tamil Nadu youth to Islamic State operatives abroad.

iv. Media and Social Media Manipulation

Narratives today are as important as operations. Extremists exploit social media algorithms, memes, reels, and deepfake videos to glorify militancy and delegitimise the state. Platforms amplify such content at scale, shaping perceptions faster than official narratives can respond.

Indian Example: Khalistani revivalists using YouTube, Instagram, and even Spotify playlists to circulate imagery and speeches glorifying Jarnail Singh Bhindranwale.

v. Drones and Commercial Technology

Low-cost drones and dual-use commercial tools provide terrorists with unprecedented logistical capacity. They enable smuggling of arms and narcotics, reconnaissance, and even aerial strikes—bypassing traditional border controls.

Indian Example: Pakistan-based handlers using drones to deliver weapons and drugs into Punjab, with several consignments intercepted by the Border Security Force.

vi. Lawfare and Human Rights Shields

Terrorist networks increasingly weaponise legal systems and human rights platforms to obstruct state action. Court petitions, procedural delays, and appeals to international forums provide both legitimacy and breathing space for extremist actors.

Indian Example: So-called "urban Naxal" networks filing public interest litigations and using human rights discourse to shield sympathisers, framing counter-insurgency as state repression.

vii. Ideological Warfare

At the heart of hybrid terrorism lies the battle of ideas. Extremists reframe grievances and identity politics into compelling narratives that mobilise sympathy at home and abroad. Digital "toolkits"

globalise local protests, while selective framing of events transforms domestic unrest into international campaigns.

Indian Example: The Shaheen Bagh protests reframed through international digital toolkits, which positioned them as part of a global struggle against authoritarianism, amplifying their traction across diasporic and activist networks.

c. Emerging Trends in Global and Indian Terrorism

i. Rise of Lone-Wolf Terrorists

The archetype of the organised cell is giving way to self-radicalised individuals who act without direct organisational affiliation. These lone wolves are extremely difficult to detect, as they leave minimal logistical or financial footprints.

Case in India: In 2020, an Islamic State–inspired youth in Uttar Pradesh was arrested despite having no direct links to any formal group. His radicalisation, planning, and attempted mobilisation occurred entirely in isolation.

ii. Digital-First Radicalisation

Radicalisation journeys increasingly begin—and often conclude—online. Platforms such as Instagram, YouTube, and Telegram have become accelerators, turning reels, sermons, or memes into recruitment pipelines. The digital ecosystem provides anonymity, speed, and amplification, allowing extremist ideology to spread like contagion.

Case in India: Several youth from Kerala were recruited into the Islamic State entirely through online exposure, without physical recruiters or organisational contact.

iii. State-Backed "Plausible Deniability" Warfare

Hostile states weaponise terrorism with increasing sophistication, employing proxies, hackers, or information networks to destabilise rivals while denying responsibility. This grey-zone warfare allows aggression without triggering open retaliation.

Case in India: Pakistan's enduring patronage of Lashkar-e-Taiba and Jaish-e-Mohammed exemplifies this model. Allegations of Chinese information operations on Indian social media platforms highlight how the strategy extends into digital influence campaigns.

iv. Psychological and Perception Warfare

The conflict theatre is no longer the battlefield alone but also the minds of populations. Terrorism increasingly seeks to erode morale, unity, and institutional trust, often by reframing security operations as repression. The aim is not territorial control but delegitimisation of the state.

Case in India: Videos of security encounters in Jammu and Kashmir have been reframed by extremist networks to portray state brutality, fuelling cycles of anger and alienation.

v. Exploitation of Democratic Platforms

Extremist sympathisers often hide behind the veil of dissent, exploiting democratic spaces such as protest sites, university campuses, and NGOs. These platforms become channels for seeding ideology, recruiting youth, and crafting anti-state narratives. This blurs the line between legitimate activism and radicalisation, complicating counter-terrorism efforts.

Case in India: Maoist literature has been recovered from university networks, while radical speeches have surfaced in student circles under the guise of academic or cultural discourse.

Conclusion

The new battlefield of terrorism requires neither territory nor armies—only a broadband connection, a grievance, and a receptive mind. Its tools are subtle yet potent: a drone crossing borders at night, a cryptocurrency wallet funding violence, a deepfake turning perception against the state, or a legal petition shielding extremists.

For India, the task is to evolve a counter-terrorism framework that moves beyond guns to governance, beyond force to foresight. The fight must be waged simultaneously in cyberspace, courtrooms, and the minds of citizens.

As Bruce Hoffman observed: *"The new terrorist is not just a bomber—he is a broadcaster, a hacker, and a storyteller."* Defeating him requires India to be a coder, a communicator, and a community-builder all at once.

The survey of modern terrorist tools and trends reveals a threat landscape that is dynamic, decentralised, and digitally empowered. Terrorism today infiltrates social media, courtrooms, and community spaces, far beyond traditional battlefields.

For India, facing cross-border proxies, domestic extremists, and online radicalisation simultaneously, the challenge is uniquely complex. The next section therefore examines India's counter-terrorism framework—its legislative architecture, institutional mechanisms, intelligence-sharing systems, and international cooperation—to assess how the state adapts to this hybrid threat environment.

3.10 India's Counter-Terrorism Framework

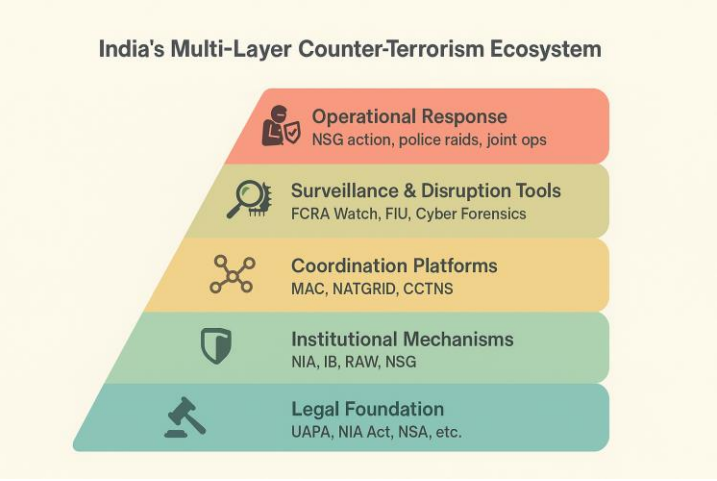
a. Introduction

India's unique geography, vast diversity, and persistent external threats make it one of the most terror-affected democracies in the world. From cross-border infiltrations in Kashmir to urban sleeper cells and digitally radicalised youth, the spectrum of threats is wide, adaptive, and constantly evolving.

A strong counter-terrorism (CT) framework is therefore essential not only to respond to attacks but also to prevent radicalisation, disrupt recruitment, track financing, and build resilience through intelligence and technology. As one analyst aptly remarked:
"India's CT framework is not just about guns and guards—it is about laws, institutions, coordination, and deterrence."

i. Legal Instruments of Counter-Terrorism

India's legislative arsenal forms the backbone of its CT efforts. Over time, these laws have expanded state capacity, though often accompanied by debates over civil liberties and judicial oversight.



- **Unlawful Activities (Prevention) Act (UAPA), 1967**: The principal anti-terror law, empowering the state to ban organisations, designate individuals as terrorists, and prosecute a wide spectrum of offences. Criticised for its low conviction rate and prolonged pre-trial detention.
- **National Investigation Agency (NIA) Act, 2008**: Created the NIA with powers to probe terror cases across state boundaries without prior consent. Strengthened federal capability, though sometimes generating centre–state friction.
- **National Security Act (NSA), 1980**: A preventive detention law permitting detention up to 12 months without charge. Effective in urgent cases but criticised for misuse and weak judicial review.

- **Maharashtra Control of Organised Crime Act (MCOCA), 1999**: State-specific law targeting the organised crime–terror nexus, especially D-Company, influential in shaping similar state frameworks.
- **Prevention of Money Laundering Act (PMLA), 2002**: Targets terror finance, hawala transactions, and NGO misuse. Effective in asset freezing but plagued by delays in trial completion.
- **Information Technology Act (Sections 66F and 69A)**: Provides the basis for tackling cyber terrorism, blocking radical websites, and enforcing online surveillance. Limited, however, by jurisdictional and global hosting challenges.

ii. Institutional Mechanisms

India's CT framework rests on a multi-layered institutional grid combining intelligence, investigation, and rapid response.

- **National Investigation Agency (NIA):** Apex body for investigating terror cases under UAPA, Arms Act, and related laws.
- **Intelligence Bureau (IB):** Primary domestic intelligence agency, tracking sleeper cells, radicalisation, and infiltration networks.
- **Research and Analysis Wing (RAW):** External intelligence arm, monitoring ISI operations, Taliban linkages, and diaspora radicalisation.
- **National Security Guard (NSG):** Elite counter-terror and hostage-rescue force. Its role in 26/11 Mumbai was a watershed in India's CT doctrine.
- **Multi-Agency Centre (MAC):** Coordination hub linking 28+ intelligence and enforcement agencies.
- **National Technical Research Organisation (NTRO):** Provides technical intelligence through satellites, drones, and cyber tracking.
- **Financial Intelligence Unit (FIU):** Tracks suspicious banking activity, shell companies, and NGO funding streams.
- **Indian Cyber Crime Coordination Centre (I4C):** Specialises in digital radicalisation, dark web monitoring, and cyber-terror tracking.

iii. Coordination and Intelligence Sharing

- **MAC and Subsidiary MACs:** Operate on a hub-and-spoke model, linking central agencies with state police and CAPFs.
- **NATGRID (National Intelligence Grid):** Integrates 20+ databases (banking, telecom, passports, travel) for real-time suspect profiling.
- **CCTNS (Crime and Criminal Tracking Network System):** Digitally connects 15,000+ police stations, enabling biometric alerts and integrated case tracking.

iv. Financial and Tech Surveillance Tools

- **FCRA Monitoring:** Tracks foreign donations to NGOs, preventing misuse for extremist agendas.
- **FIU + Enforcement Directorate (ED):** Coordinate to disrupt hawala, terror finance, and cryptocurrency channels.
- **Cyber Forensic Labs:** Support NIA, I4C, and state police in digital evidence recovery and analysis.

Conclusion

India's counter-terrorism framework is formidable in design—anchored in strong laws, specialised institutions, technical capacity, and financial surveillance. Yet, effectiveness often falters due to inter-agency silos, centre–state frictions, low conviction rates, and difficulties in balancing security with rights.

As a maxim in counter-terrorism reminds us:
"A terror plot needs one gap to succeed. A CT system needs zero gaps to prevent it."

In the age of cyber strikes and networked radicalisation, India must evolve towards an intelligence-led, seamlessly integrated, and rights-respecting ecosystem. The real strength of counter-terrorism lies not only in eliminating threats but in safeguarding democracy while doing so.

India's counter-terrorism framework reflects decades of institutional learning—from the NSG's creation post-1984, to the enactment of UAPA and PMLA, and from intelligence platforms like MAC and NATGRID to cyber-focused centres like I4C. On paper, the architecture appears robust. But the true test lies in its execution.

In practice, India's CT ecosystem faces persistent challenges: centre–state tensions, low conviction rates, overlapping jurisdictions, grassroots resource gaps, and human rights concerns. Terrorist groups thrive on exploiting precisely these fissures.

The next section therefore undertakes a critical appraisal of the challenges in India's counter-terrorism framework—legal, operational, political, and ethical—that undermine effectiveness. Only by addressing these can India move toward a truly seamless and resilient CT model.

3.11 Challenges in India's Counter-Terrorism (CT) Framework

a. Introduction

India confronts one of the world's most complex terror landscapes—ranging from cross-border jihadist infiltration in Jammu and Kashmir to Maoist insurgency in the heartland, from Khalistani revivalism to digital radicalisation of urban youth. Over the years, the country has built a formidable counter-terrorism (CT) architecture, anchored in strong laws, elite institutions, and sophisticated surveillance tools.

Yet, the effectiveness of this system is undermined by uneven implementation, coordination gaps, and the demands of a rapidly digitising threat environment. Fragmentation, federal friction, and manpower deficits often weaken India's response, reminding us that robust structures on paper do not always translate into seamless execution on the ground.

b. Challenges in India's Counter-Terrorism Framework

i. Overlapping Jurisdictions and Turf Wars

The multiplicity of agencies—IB, NIA, State Police, ATS, DRI—creates duplication, delays, and even operational compromises. Competing mandates mean suspects may be pursued by different agencies simultaneously, eroding surprise and exposing intelligence.

Illustrative Example: In 2021, parallel operations by the NIA and state police in West Bengal created confusion, exposed operational details, and compromised secrecy—opportunities which terror networks are quick to exploit.

ii. Lack of Statutory Status for Intelligence Bodies

Key intelligence agencies such as the IB, MAC, and NSCS lack statutory foundations. Operating in legal grey zones, they face contested jurisdictions, minimal parliamentary oversight, and weak accountability. Without legislative clarity, their mandates remain open to interpretation, undermining both operational effectiveness and democratic legitimacy.

iii. Federal Friction between Centre and States

"Police and law and order" are state subjects under the Constitution. Central intervention—especially by the NIA or CBI—is often seen as encroachment on state autonomy. This leads to political pushback, slowed investigations, and fractured intelligence sharing.

Illustrative Example: States such as West Bengal and Maharashtra have resisted NIA involvement in sensitive cases, delaying coordinated action and weakening national security unity.

iv. Slow Investigations and Low Conviction Rates

Despite strong laws such as UAPA, conviction rates remain poor—around 27% (NCRB 2022). Reasons include:

- weak evidence collection,
- delays in forensic analysis,
- hostile witnesses, and
- inadequately trained prosecutors.

Long delays undermine deterrence and fuel extremist narratives of victimisation, eroding public trust in CT laws.

v. Human Resource Gaps

Modern terrorism demands specialist expertise that India lacks in adequate numbers:

- cyber specialists,
- language experts: Arabic, Pashto, Mandarin
- financial intelligence analysts capable of tracing hawala and crypto flows.

Local police, often first responders, are ill-trained in OSINT, crypto-tracing, or drone forensics—leaving a mismatch between terrorist sophistication and domestic capacity.

vi. Deficits in Tech and Forensic Infrastructure

Extremists exploit drones, encrypted devices, and blockchain transactions, but only a handful of Indian labs are capable of investigating these. Many state ATS units still rely on outdated systems, making them reactive rather than anticipatory.

Emerging Needs: Drone forensics, advanced device decryption, and blockchain analytics remain critical gaps.

vii. Poor Inter-Agency Data Integration

Projects such as NATGRID, CCTNS, and I4C remain under-implemented. Databases lack standardisation, legacy silos persist, and real-time police station updates are inconsistent. Information exists in abundance, but actionable intelligence often arrives too late to prevent attacks.

viii. Weak Strategic and Narrative Capability

India's CT strategy remains heavily kinetic—focused on arrests, seizures, and bans. While effective tactically, it has struggled to delegitimise the ideas that fuel extremism. Counter-narratives, academic partnerships, or systematic psychological operations are underdeveloped. Extremists thus retain dominance in the ideological and perceptional battlefield, both online and offline.

Conclusion

India's CT framework is strong in structure but weak in synergy. The nation does not lack laws, institutions, or surveillance tools; what it lacks is coordination, speed, and imagination. Legal

strength must be matched with operational integration, digital-age manpower, and narrative dominance.

As former NSA Shivshankar Menon observed:
"We are not short on laws or agencies—but on coordination, speed, and imagination."

The war on terror must therefore evolve from reactive defence to proactive deterrence, building an ecosystem that is as smart, seamless, and rights-respecting as it is strong.

The challenges outlined above reveal how India's counter-terrorism framework, despite its robust architecture, struggles with coordination, capacity, and narrative dominance. Yet terrorism is not confined within India's borders. Its networks of finance, ideology, training, and propaganda are deeply transnational—linking lone actors in India to handlers in Pakistan, funding streams in Dubai, and propaganda hubs in Canada.

This interconnected reality means that India's CT strategy cannot remain inward-looking. Domestic reform must be complemented by robust international cooperation—through intelligence sharing, financial monitoring, diplomatic pressure, and joint operations under multilateral frameworks.

The next section therefore turns to Global Cooperation and India's Counter-Terrorism Strategy, examining how India leverages bilateral, regional, and multilateral partnerships to strengthen security, shape global norms, and counter the transnational dimensions of terrorism.

3.12 Global Cooperation and India's Counter-Terrorism Strategy

a. Introduction

Terrorism in the twenty-first century is transnational, digital, decentralised, and privately financed. A single plot may be conceived in Pakistan, funded through Dubai, radicalised via YouTube servers in the United States, and executed in Mumbai. This interconnectedness renders national boundaries increasingly irrelevant for both detection and disruption.

As one analyst aptly noted: *"When a YouTube sermon radicalises a youth in Kerala to fight in Syria, counter-terrorism must be global, not local."*

For India, global partnerships are no longer optional—they are indispensable multipliers of national security. Whether it is tackling cross-border safe havens, dismantling financial pipelines, or combating digital radicalisation hosted on foreign servers, India's ability to protect its citizens now depends on leveraging international cooperation as effectively as domestic instruments.

b. Why India Needs Global Counter-Terrorism Partnerships

Several structural features of modern terrorism compel India to seek robust international coordination:

- **Terror Financing:** Funds move through cryptocurrency, hawala networks, and layered shell companies across multiple jurisdictions, making purely domestic tracking insufficient.
- **Safe Havens:** States such as Pakistan and Afghanistan continue to shelter fugitives like Dawood Ibrahim and Hafiz Saeed, undermining India's security.

- **Diaspora Misuse:** Radical diaspora groups in Canada, the UK, and the US exploit free speech protections to promote violent separatism, as seen with Sikhs for Justice and "Khalistan 2.0" campaigns.
- **Cyber and Encrypted Apps:** Extremist propaganda often resides on servers abroad, shielded by foreign data laws. Delays in takedowns by platforms like Telegram or Twitter weaken India's response.
- **Global Propaganda:** Narratives such as *"Hindutva fascism"* or *"Free Kashmir"* are amplified by NGOs, academics, and diaspora influencers, complicating India's diplomatic space.

India's internal security, therefore, is increasingly a function of external partnerships, legal frameworks, and diplomatic leverage.

c. Key Global Platforms and India's Role

Institution / Mechanism	Purpose	India's Role
UN Counter-Terrorism Committee (UNCTC)	Coordinates global anti-terror policy, maintains sanctions lists	Chaired in 2022; pushed reforms to target Pakistan-based groups
FATF (Financial Action Task Force)	Sets norms to combat terror financing and money laundering	Instrumental in Pakistan's greylisting (2018–22), disrupting LeT/JeM funding
Interpol	Issues Red Notices and coordinates global arrests	Used to pursue fugitives like Dawood Ibrahim and Zakir Naik
SCO – Regional Anti-Terrorist Structure (RATS)	Joint counter-terror drills and intelligence sharing in Eurasia	Hosted SCO-RATS military exercises at Manesar
BRICS CT Working Group	Joint statements and coordination	Consistently pressed for naming LeT and JeM, resisting "double standards"
Quad	Cybersecurity, maritime security, critical infrastructure	Co-developing CERT frameworks and undersea cable security

d. Bilateral and Multilateral Partnerships

- **United States:** Homeland Security dialogue, financial intelligence sharing, and cyber forensics cooperation.
- **France:** Joint counter-radicalisation programmes, intelligence training, and CT exercises.
- **Russia:** Collaboration on narco-terror financing and arms smuggling routes via the Northeast.
- **Australia:** Indo-Pacific drills, AI-driven radicalisation monitoring.
- **Israel:** Advanced surveillance, UAV technology, and counter-terror training—a model of *"tech-driven resilience."*
- **Gulf Cooperation Council (GCC) States:** Real-time intelligence on IS-linked diaspora; deportation of Indian-origin fugitives.
- **Bangladesh:** Joint operations against ULFA; coordinated border management.
- **Myanmar:** Targeting NSCN-K and dismantling drug–gun–terror nexuses in the Northeast.

e. India's Diplomatic Response After Major Attacks

- **26/11 Mumbai Attacks (2008):** India submitted dossiers to Pakistan, leveraged FATF and UNSC to isolate LeT and ISI handlers, and deepened CT cooperation with the US and Israel.
- **Pulwama Attack (2019):** Responded with Balakot airstrikes, invoked international law doctrines of self-defence, and neutralised criticism through proactive diplomatic outreach.

- **Khalistani Revival (2020s):** Issued notes to Canada and the UK, exposed Sikhs for Justice's funding networks, and built dossiers highlighting the misuse of foreign soil for anti-India activities.

f. Strategic Shifts in India's Counter-Terrorism Diplomacy

India's global CT posture has shifted from being seen as a defensive victim to an assertive disruptor. Six key shifts illustrate this transformation:

- **From Reactive Protest to Proactive Dossier Diplomacy:** Moving beyond rhetoric, India now furnishes actionable intelligence and detailed dossiers to partners.
- **From Defence-Only to Integrated Cyber, Finance, and AI Surveillance:** Greater emphasis on FATF cooperation, financial intelligence, and digital surveillance (I4C).
- **From UN-Centric to Multi-Track Engagement:** Supplementing UN with FATF, Interpol, SCO-RATS, and bilateral partnerships (Israel, UAE, France).
- **From Physical Security to Narrative and Information Warfare:** Recognising propaganda as a weapon, India monitors disinformation, diaspora activism, and online radicalisation.
- **From State-to-State Channels to Diaspora Engagement:** Leveraging consulates, G20 platforms, and diaspora networks for counter-radicalisation abroad.
- **From Non-Confrontational Diplomacy to Naming and Shaming:** India now openly calls out obstructive states, e.g., China blocking UNSC terror designations.

This marks India's transition from a reactive stance to agenda-setting in global CT diplomacy.

g. Challenges in India's Global Counter-Terrorism Cooperation

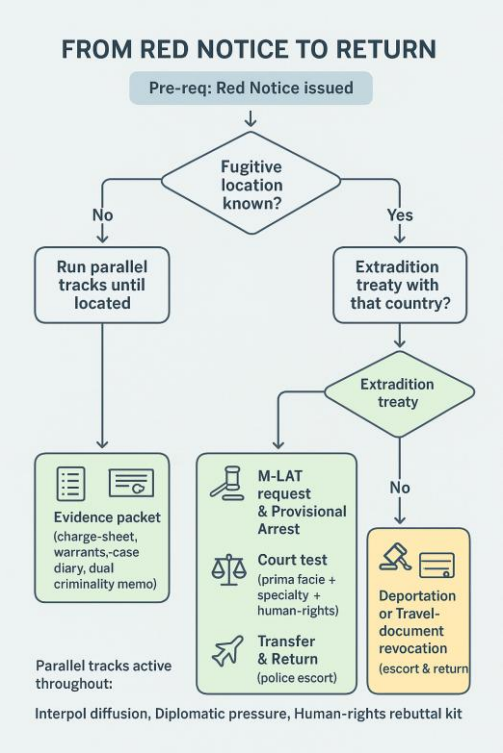
Despite progress in building partnerships, several structural and political obstacles continue to limit the effectiveness of India's global CT diplomacy. These challenges highlight the gap between the promise of international cooperation and its on-ground performance.

i. Selective Morality and Geopolitical Hypocrisy

Counter-terrorism is often applied through the prism of geopolitics rather than principle. Nations pursue selective standards, shielding extremist actors when it aligns with their strategic interests.

- China has repeatedly blocked India's attempts in the UN Security Council to sanction Pakistan-based leaders such as Masood Azhar.
- Several Western democracies overlook diaspora-based radicalism under the cover of free speech, enabling groups such as Sikhs for Justice to mobilise openly.

Impact: This selective morality erodes the credibility of global CT regimes and perpetuates safe havens for extremists.



ii. Absence of a Universal Definition of Terrorism

The global debate remains mired in the unresolved question of whether "freedom fighters" can be equated with terrorists. India's Comprehensive Convention on International Terrorism (CCIT), first tabled in 1996, has stalled for decades due to such disagreements.

Impact: The lack of consensus allows states such as Pakistan to exploit definitional ambiguities, portraying cross-border militancy as *"legitimate resistance."* Without a universal definition, enforcement remains inconsistent and politicised.

iii. Tech Platform Impunity and Legal Shields

Digital platforms remain major enablers of radicalisation yet enjoy significant legal protection in Western jurisdictions.

- In the United States, Section 230 of the Communications Decency Act shields platforms from liability for user-generated content.
- In Europe, strong intermediary protections slow down enforcement.

Impact: Extremist propaganda, deepfakes, and hate speech spread faster than regulators can respond, allowing digital radicalisation to outpace international CT cooperation.

iv. Judicial Non-Cooperation in Extradition

Extradition remains a recurring stumbling block in India's pursuit of justice. High-profile fugitives—including Dawood Ibrahim, Zakir Naik, and Tiger Hanif—have evaded repatriation for years. Host states frequently cite human rights concerns, political sensitivities, or procedural loopholes to deny requests.

Impact: The inability to secure extradition weakens deterrence, emboldens extremist networks, and undermines India's credibility in enforcing accountability beyond its borders.

h. Way Forward for India's Global Counter-Terrorism Strategy

To consolidate its role as a proactive CT actor, India must deepen and innovate its global approach:

- **Push for UN CCIT:** Renew momentum for the Comprehensive Convention on International Terrorism, align with Global South partners, and press for a neutral definition covering both state and non-state actors.
- **Strengthen Financial Surveillance Networks:** Expand partnerships with FATF, SEBI, RBI, FIU-IND; establish FATF-style frameworks in South Asia, the Gulf, and Africa; and enhance traceability of cryptocurrencies and hawala chains.
- **Export the India Stack as a Digital CT Tool:** Share platforms like Aadhaar, UPI, DigiLocker, and e-KYC with partner nations to eliminate ghost beneficiaries and block funding leaks.
- **Develop AI Surveillance for Radicalisation:** Collaborate with Quad, Israel, and EU partners to co-develop AI/ML systems for real-time monitoring of extremist chatter, darknet forums, and facial recognition—while embedding safeguards for ethical use.
- **Institutionalise Diaspora Intelligence Cells:** Establish dedicated diaspora watch units in Indian embassies, tasked with tracking extremist messaging, following funding flows, and engaging moderate diaspora leaders to isolate fringe actors.

Conclusion

In an era where radicalisation is transmitted via cloud servers, money crosses borders in seconds, and attackers train in one country to strike in another, national security has become inseparable from international cooperation. No nation can confront terrorism alone; every bilateral tie, multilateral forum, and technology platform becomes part of the battlefield.

India's evolution—from a defensive victim to an assertive disruptor—signals growing strategic maturity. Yet sustaining this momentum will require sharper diplomacy, faster intelligence sharing, and legal innovation that matches the speed of transnational terror.

As External Affairs Minister Dr. S. Jaishankar has emphasised: *"Just as terror is borderless, so must be our resolve."*

The study of terrorism and radicalisation revealed how India's internal security is increasingly shaped by hybrid threats that blend violence, ideology, and technology. Yet these threats do not emerge in isolation. They are often fuelled, financed, or facilitated by actors beyond India's borders. State sponsors provide safe havens and strategic direction, while non-state networks exploit cyberspace, narcotics, and diaspora platforms to penetrate India's internal fabric.

This convergence blurs the line between internal and external security. A lone wolf radicalised in Kerala may be inspired by content produced in Syria, financed via Dubai, and legitimised by diaspora activism in Canada. Similarly, insurgencies in the Northeast or Maoist zones often find sustenance in cross-border sanctuaries and illicit supply chains.

To fully grasp India's security landscape, it is therefore necessary to examine the role of external state and non-state actors in shaping domestic threats. The next chapter turns to this crucial theme—exploring how geopolitics, proxy warfare, organised crime, and transnational ideologies intersect with India's internal security challenges, and how the state must adapt to defend sovereignty in an interconnected world.

Chapter 4. Role of External State & Non-State Actors in Internal Security Threats

4.1 Role of External State

a. Introduction

In the evolving landscape of India's internal security, not all threats are indigenous in origin. Some are carefully scripted and orchestrated by external state actors who prefer to wage war without formally declaring it. These states weaponise proxies, technology, identity politics, disinformation, and economic subversion to achieve what conventional war cannot—destabilise India from within while avoiding direct confrontation.

External state-sponsored interference has become the quintessential weapon of asymmetric conflict in the twenty-first century. It is cheap, deniable, and politically expedient. Instead of tanks, it uses Telegram groups; instead of armies, it deploys NGOs, drones, and hashtags. Hostile states such as Pakistan and China systematically exploit India's democratic strengths—its open borders, press freedom, pluralistic society, and decentralised politics—turning them into vulnerabilities.

As one Indian analyst observed: *"You don't need to invade India to hurt it. You just need to fund a madrasa, drop a drone, pay a YouTuber, or protect a fugitive."*

This section explores why external states interfere in India's internal security, the tools they deploy, and the country-specific patterns of threat that compel India to recalibrate its security architecture for an age of "warfare without war."

b. Why Do External States Interfere in Internal Security?

When direct war is costly, risky, or diplomatically unacceptable, states turn to sub-conventional means, exploiting fault lines of religion, caste, ethnicity, and underdevelopment. Their objectives are clear:

- **Bleeding through Low-Cost Warfare**
  - Pakistan's doctrine of *"Bleed India with a Thousand Cuts"* rests on training, financing, and sheltering terrorist groups that attack Indian targets.
- **Undermining Unity and Democratic Stability**
  - Hostile propaganda campaigns amplify divisive narratives, exploiting India's pluralism through digital platforms and diaspora activism.
- **Retaliation for Geopolitical Setbacks**
  - China has covertly aided insurgent groups in India's Northeast, particularly in moments of heightened border tension, such as post-Doklam or Galwan.
- **Influencing Borderland Politics**
  - Neighbouring states like Myanmar and Bangladesh have historically provided shelter or transit corridors for insurgent groups in the Northeast.

- **Using Internal Chaos as Diplomatic Leverage**
    - Pakistan seeks to internationalise the Kashmir issue at the UN, while China portrays instability in India as justification for its own hardline policies in Tibet and Xinjiang.

c. Country-Wise Threat Mapping

Country	Mechanism of Threat	Details
Pakistan	State-sponsored terrorism, ISI financing, radicalisation, drone-based infiltration	Groups like JeM and LeT, along with Khalistani outfits, are trained in Pakistan-occupied Kashmir. Drones drop AK-47s, heroin, and counterfeit currency into Punjab. Radical preachers and influencers often operate with Gulf-based financial backing.
China	Proxy insurgent support, cyber operations, information warfare	Historically extended covert support to ULFA and NSCN; conducted cyberattacks on Indian infrastructure (e.g., 2020 Mumbai power grid incident); deployed disinformation campaigns during the Galwan clashes.
Bangladesh	Border crime hubs, Islamist spillovers, safe havens (historically)	Earlier provided sanctuary to ULFA and other insurgents, though cooperation improved under Sheikh Hasina. Challenges persist in illegal immigration and Fake Indian Currency Note (FICN) flows.
Myanmar	Safe havens for insurgents, porous borders, arms and drug trafficking	Groups such as NSCN-K, ULFA, and PLA maintain bases in the Sagaing region. Arms and narcotics from the Golden Triangle fuel unrest in the Northeast. Post-2021 coup instability has further reduced cooperation.

External interference is not merely an external affairs issue—it is a direct assault on India's internal cohesion. By combining terrorism, cyber operations, and narrative warfare, hostile states aim to exhaust India's resources, erode trust, and fracture unity.

d. Tools Used by Hostile States

The hallmark of modern state-sponsored interference is its reliance on asymmetric, deniable, and low-cost tactics that yield high disruption. Hostile states employ a toolkit that blends ideology, finance, technology, and geography.

- **Terror Proxies**
    - Pakistan's reliance on non-state actors such as LeT and JeM is a classic example. Training camps in PoK arm and indoctrinate cadres, enabling Islamabad to wage war by proxy while maintaining plausible deniability.
- **Digital Propaganda and Influence Operations**
    - Fake social media accounts, bot networks, AI-generated content, and diaspora-linked NGOs magnify narratives of victimhood.
    - Example: During debates on CAA and the abrogation of Article 370, Pakistani-linked accounts flooded platforms with fabricated stories designed to provoke unrest.
- **Drone-Based Supply Chains**
    - Low-cost commercial drones are now central to cross-border logistics. They deliver arms, narcotics, fake currency, and encrypted devices, particularly across Punjab and Jammu.
    - Example: ISI-backed drone drops of RDX and heroin intercepted by the Border Security Force.
- **Cyber Sabotage**

- State-linked hackers target critical infrastructure—energy grids, telecom, and financial systems—causing disruption without overt conflict.
- Example: The 2020 Mumbai power outage, attributed to Chinese-linked groups, demonstrated cyber warfare as coercive signalling.

- **Economic Subversion**
  - Tools include circulation of FICN, crypto-based financial transfers, and gold smuggling. These destabilise the economy while simultaneously funding extremism.
  - Routes through Nepal and Bangladesh are routinely used to push counterfeit notes into Uttar Pradesh, West Bengal, and Kerala.
- **Religious Radicalisation**
  - Funds funnelled into madrasas, clerics, and identity-based organisations promote sectarianism and separatism.
  - Example: Spread of Wahhabi–Salafi influence in Kerala, with Gulf remittances diverted towards extremist causes.

Conclusion

Modern conflict has blurred the boundary between war and peace. States no longer need to deploy armies across borders; they can instead arm the actorless, weaponise information, and radicalise identities. This form of grey-zone interference forces India to adapt its doctrine for an era where the aggressor is invisible, the battlefield is psychological, and legitimacy is as important as firepower.

India's response must therefore rest on a doctrine of "asymmetric resilience." This means integrating technology-driven intelligence, cyber preparedness, financial surveillance, and community resilience with diplomatic pressure and federal synergy. Just as nuclear strategy defined the twentieth century, asymmetric resilience must become the defining concept of India's internal security posture in the twenty-first.

As counter-terrorism expert Ajai Sahni has aptly warned: *"In the age of grey-zone conflict, the line between internal disorder and external aggression is not just blurred—it is often intentionally erased."*

Yet, while hostile states like Pakistan and China often stand behind the curtain, the most visible threats to India's internal security are carried out by non-state actors. These groups—ranging from insurgents and terrorists to organised crime syndicates and radical networks—may receive foreign support, but they operate with their own motivations, hierarchies, and ecosystems.

Unlike state actors, non-state actors thrive on fluidity and deniability. They adapt quickly, blend into civilian populations, and exploit modern technologies to stay ahead of enforcement. Some, like Maoists, aim to overturn the State through ideology and guerrilla warfare. Others, like Lashkar-e-Taiba or ISIS modules, pursue religious or transnational goals. Still others, such as the D-Company, blur the line between crime and terrorism by funding violence through narcotics and smuggling.

To understand the full spectrum of India's security challenges, it is therefore necessary to turn from the external hand of hostile states to the internal and hybrid agency of non-state actors. The next section will examine how such groups shape, sustain, and complicate India's internal security environment.

4.2 Non-State Actors and Internal Security

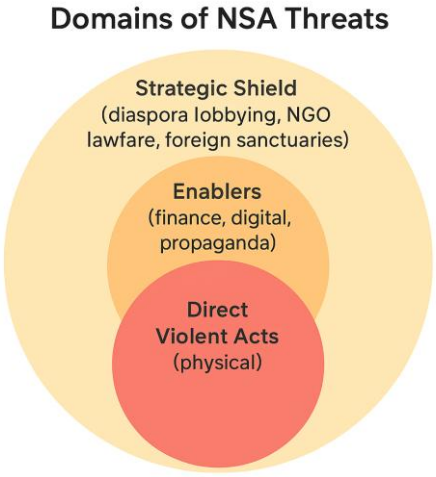
a. Introduction

Non-State Actors (NSAs) represent one of the most disruptive forces in modern security. Operating independently of sovereign governments, they lack formal authority yet wield influence capable of undermining sovereignty, legitimacy, and social cohesion. Unlike conventional adversaries in uniform, these actors exist in the shadows, moving fluidly across borders and domains.

In India, the spectrum of NSAs is particularly vast: from terrorists and insurgents to cyber hackers, narco-cartels, diaspora-funded lobbies, and civil society organisations with covert agendas. Their operations exploit the very openness of India's democratic society—its free press, plural identities, digital access, and decentralised politics.

The modern NSA does not always carry a gun. It may operate with a smartphone, an encrypted channel, a deepfake video, or even a litigation strategy in the name of rights. They thrive in grey zones—between activism and subversion, charity and radicalisation, privacy and propaganda—where law struggles to distinguish dissent from destabilisation.

As one security analyst observed: *"Today's wars are not always fought between armies—but between ideas, networks, and non-state actors who reject the rules of the game."*



b. Types of Non-State Actors Threatening India

Type	Key Characteristics	Examples
Terrorist Organisations	Use violence for political or religious ends; funded via illicit networks	Lashkar-e-Taiba (LeT), Jaish-e-Mohammed (JeM), Islamic State – Khorasan Province (ISKP), Students Islamic Movement of India (SIMI), Indian Mujahideen (IM)
Insurgent / Militant Groups	Armed rebellion exploiting ethnic or regional grievances	NSCN (K), ULFA, PLA, CPI (Maoist)
Organised Crime Syndicates	Transnational illegal activity, often symbiotic with terror networks	D-Company, narco-cartels, gold smuggling rings
Cyber Hackers and Darknet Cells	Digital espionage, infrastructure disruption, radicalisation	North Korea-linked Lazarus Group, freelance hacktivists
Narco-Terror Networks	Use drug trafficking to fund insurgency and weaken societies	Golden Crescent and Golden Triangle syndicates
Diaspora-Based Radical Outfits	Mobilise funds, disinformation, and political pressure abroad	Sikhs for Justice (SFJ), radical Islamic charities with opaque funding
NGO Fronts and Civil Society Shells	Provide legal or intellectual cover for extremist ideologues	Select NGOs flagged under FCRA scrutiny

c. Case Insights

The disruptive capacity of Non-State Actors becomes clearer through specific episodes that highlight their methods, networks, and impact:

- **Mumbai Underworld and ISI: The 1993 Blasts**
  The D-Company collaborated with Pakistan's Inter-Services Intelligence (ISI) to smuggle RDX

into India and train operatives abroad. This nexus culminated in the coordinated serial bombings across Mumbai, marking one of the deadliest examples of crime–terror collaboration in India's history.

- **NSCN (K) Bases in Myanmar**
  Insurgent groups such as the NSCN (Khaplang) exploited the porous Indo–Myanmar border, tribal kinship across frontiers, and Myanmar's limited state control in the Sagaing region. These sanctuaries enabled militants to regroup, train, and evade Indian jurisdiction, prolonging insurgencies in the Northeast.
- **ISKP Online Recruitment**
  The Islamic State Khorasan Province (ISKP) demonstrated the power of digital radicalisation by recruiting youth in Kerala and Telangana through Telegram, WhatsApp, and online propaganda magazines. This showed how extremist pipelines no longer depend on physical camps or recruiters—radicalisation can now unfold entirely in cyberspace.
- **Sikhs for Justice (SFJ) and Diaspora Disinformation**
  The diaspora-based outfit Sikhs for Justice (SFJ) launched "Referendum 2020" campaigns abroad, leveraging social media to project separatism as a democratic movement. Its online disinformation targeted Punjab's youth, fuelling pro-Khalistan sentiment while exploiting protections for free speech in Western democracies.

Conclusion

Non-State Actors are the new-age antagonists of internal security. Unbound by geography, morality, or international law, they wage war not just with violence but also with virality, identity politics, and deception. For India, they represent a particularly complex challenge because they exploit the freedoms of democracy while rejecting its responsibilities.

Neutralising such actors requires far more than kinetic force. It demands:

- intelligence integration to map their shifting networks,
- narrative dominance to counter their propaganda,
- digital vigilance to track their online influence,
- financial tracing to choke illicit flows, and
- legal innovation to deny them legitimacy under the garb of rights or activism.

As former RAW chief Vikram Sood aptly warned: *"When the enemy has no flag, no face, and no fear—strength alone is not enough. States must out-think as much as out-fight."*

The mapping of NSAs has shown how groups—whether terrorists, insurgents, diaspora lobbies, or narco-cartels—exploit India's vulnerabilities. Yet they rarely act in isolation. More often, they function as proxies of hostile states, providing the perfect instruments for indirect conflict.

This convergence of state sponsorship and non-state execution lies at the heart of asymmetric warfare. It has shifted the battlefield from conventional military fronts to villages, cities, cyberspace, and even international narratives. For India, this means that internal security cannot be disentangled from external rivalries. A drone dropping narcotics in Punjab, a cyber-attack on a Mumbai power grid, or a propaganda campaign launched from Canada—all belong to the same continuum of proxy conflict.

The next section therefore turns to Asymmetric Warfare and Proxy Wars—examining how adversaries blend terrorism, cyber operations, disinformation, and organised crime into a coherent strategy of low-cost, high-deniability disruption against India.

4.3 Asymmetric Warfare and Proxy Wars

a. Introduction

Asymmetric warfare and proxy wars represent the modern grammar of conflict—where strength does not guarantee victory, and weakness does not preclude resistance. In this arena, battles are not fought through tanks and armies alone but through subversion, sabotage, and narrative control.

For India, these strategies lie at the heart of internal security challenges, as hostile states and non-state actors increasingly blend technology, ideology, and organised crime to destabilise from within.

b. What is Asymmetric Warfare?

Asymmetric warfare refers to conflict in which the weaker side refuses to engage by the stronger opponent's rules. Instead of matching conventional might, it relies on unconventional methods—guerrilla ambushes, improvised explosive devices (IEDs), cyberattacks, drones, or propaganda—to exploit vulnerabilities.

It is, in essence, a war between unequals: one side possessing superior force, the other wielding superior ingenuity.

c. What are Proxy Wars?

Proxy wars occur when external powers pursue strategic objectives indirectly, by arming, funding, or guiding actors within another state while officially denying involvement.

- For the sponsor: Proxy warfare provides deniability and low-cost leverage.
- For the proxy: It ensures resources, legitimacy, and protection.

Proxy wars are thus the invisible hand of foreign policy—pulling strings without ever stepping on stage.

d. Key Characteristics of Asymmetric Warfare

- **Unconventional Tactics**
  Guerrilla ambushes, suicide bombings, IEDs, drone drops, and cyber intrusions bypass traditional force-on-force engagement.
  - *Examples:* Maoist ambushes in Dandakaranya; drone-dropped arms in Punjab; the 2020 cyber sabotage of Mumbai's power grid.
- **Non-State Actors as Proxies**
  Hostile states outsource disruption to militant groups, providing training, finance, and political cover.
  - *Examples:* Pakistan's ISI support to LeT and JeM; China's historical links with ULFA and NSCN(K).
- **Use of Terrain and Anonymity**
  Dense jungles, mountainous borders, urban slums, refugee camps, and cyberspace offer natural shields.
  - *Examples:* Maoists entrenched in Chhattisgarh forests; Islamist sleeper cells operating quietly in metros.
- **Psychological and Ideological Warfare**
  The battle is fought as much in the mind as on the ground. Martyrdom glorification, deepfake videos, and disinformation erode trust and provoke unrest.
  - *Example:* Online glorification of slain militants during Kashmir unrest.
- **Low-Cost, High-Impact Operations**
  Minimal investments generate disproportionate disruption.
  - *Examples:* Crude IEDs paralysing convoys; cryptocurrency-funded plots; social-media campaigns sparking riots in Delhi or Bengaluru.

- **Adaptability and Agility**
  Asymmetric actors are nimble, shifting platforms and tactics rapidly.
    - *Examples:* Migration from Telegram to Threema; shift from drones to underground tunnels for supply.
- **Integration with Information Warfare**
  Kinetic attacks are paired with cognitive disruption. Hashtags, toolkits, and curated propaganda amplify violence into national and international campaigns.
    - *Examples:* Diaspora-driven hashtag activism during Kashmir unrest.

Conclusion

Asymmetric warfare and proxy wars redefine conflict. The enemy is not always a soldier in uniform, but a network of narratives, shadows, and code. For India, the battlefield is now perpetual and borderless:

- drones deliver arms,
- algorithms spread propaganda,
- proxies act as the surrogates of hostile states.

Victory in such wars is not measured by territory captured but by legitimacy preserved and narratives sustained.

As General David Petraeus observed: *"Victory in asymmetric war doesn't go to the side with more firepower—but to the one with faster adaptation and stronger narratives."*

If asymmetric warfare explains the *"how"* of unconventional conflict and proxy wars expose the *"who"* behind them, then information warfare reveals the "where"—the invisible battlespace of ideas, perception, and legitimacy.

Unlike proxy groups armed with guns or drones, information warriors operate with data, narratives, and networks. Their task is not to capture territory but to capture belief—to weaken public trust, delegitimise state authority, and polarise communities.

From covert espionage that plants moles in institutions, to ideological infiltration in universities, to online disinformation campaigns run from foreign servers, adversaries now treat information as a weapon system. In this theatre, victories are won not by firepower but by framing, where one viral video or deepfake can erode years of institutional credibility.

It is in this context that the next section turns to Information Warfare—mapping how covert espionage, ideological control, and digital narratives are shaping India's internal security challenges in the twenty-first century.

4.4 Information Warfare: Covert Espionage, Ideological Control, and Online Narratives

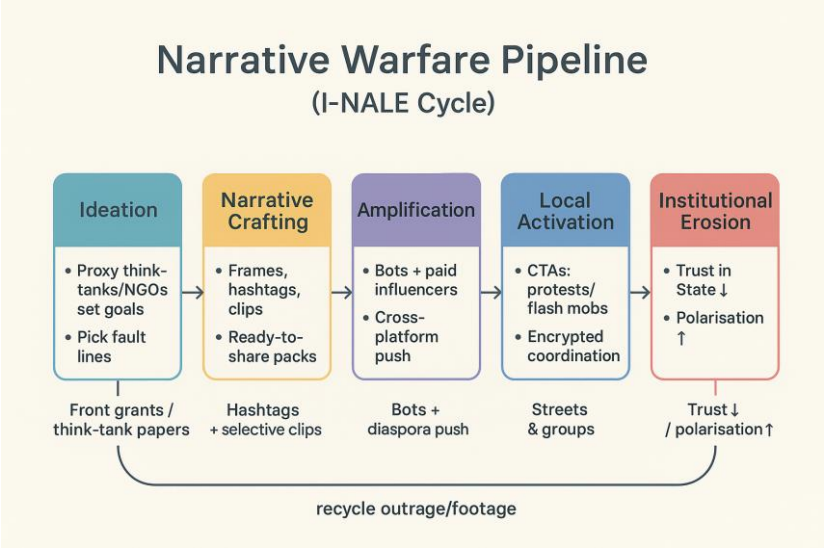
a. Introduction

In the twenty-first century, the battlefield of conflict is no longer limited to terrain, borders, or military installations. It has decisively shifted to the domain of perception and belief. Information warfare represents this transformation: campaigns that manipulate trust, legitimacy, and identity without relying on physical violence. For adversaries, these are low-cost, deniable, and highly effective operations that strike at the psychological and cognitive foundations of society.

In India's case, information warfare seeks to fracture internal cohesion, erode institutional credibility, and weaken the democratic consensus that binds its diverse population. These operations thrive in the open ecosystems of democracy—media, academia, culture, and social media—where narratives travel faster than facts and emotion often outpaces reason. The ability to persuade, mislead, and polarise has, in many cases, proved more damaging than the ability to invade.

b. Core Components of Information Warfare

Information warfare is waged through multiple, often overlapping, instruments. Each exploits vulnerabilities in India's social, political, and technological environment.



i. Covert Espionage and Infiltration

- **Description:** Traditional espionage remains central to information warfare. External actors insert agents, cultivate insiders, or use covert collaborations to extract information and shape decision-making.
- **Indian Examples:** Honey traps targeting military personnel; research collaborations masking data-gathering; insider leaks from government ministries and defence institutions.

ii. Ideological Control and Subversion

- **Description:** Adversaries promote radical or disruptive ideologies to delegitimise democratic processes, fuel unrest, and erode trust in governance. This may be religious extremism, left-wing radicalism, or even ultra-nationalist mobilisation.
- **Indian Examples:** Urban Naxal narratives that justify violence as resistance; foreign-funded NGOs opposing development projects under the cover of human rights activism; circulation of separatist propaganda in universities.

iii. Online Narratives and Digital Manipulation

- **Description:** Social media and digital platforms have become the frontline of narrative battles. Bot networks, troll farms, fake news, and deepfakes are deployed to create outrage, spread confusion, and discredit institutions.
- **Indian Examples:** Anti-India hashtag campaigns during CAA/NRC protests; misinformation circulated during the Galwan border standoff; viral propaganda videos amplifying communal tensions.

iv. Diaspora-Driven Information Campaigns

- **Description:** Radical diaspora groups mobilise resources, lobbying power, and global visibility to influence India's internal discourse from abroad.
- **Indian Examples:** Sikhs for Justice (SFJ) organising "Referendum 2020" campaigns from Canada and the UK; diaspora-backed protests portraying Indian laws as repressive or authoritarian.

v. Academic and Media Capture

- **Description:** Covert sponsorship of research projects, think tanks, and media platforms is used to shape intellectual and policy narratives. These efforts often reframe counter-terrorism or governance measures as oppressive.
- **Indian Examples:** Select international reports branding security operations in Kashmir as "human rights violations"; academic conferences funded by overseas organisations that amplify separatist or extremist viewpoints.

c. The Influence Operations Toolkit

The arsenal of information warfare is diverse, technology-driven, and deeply psychological. These are not weapons of destruction but of deception and manipulation, making them difficult to detect yet devastating in effect.

i. Deepfakes and Synthetic Media
AI tools now fabricate convincing audio or video content that impersonates leaders, soldiers, or community figures. Unlike crude edits of the past, deepfakes are indistinguishable from reality.

- *Risk:* A fake clip of Indian Army personnel committing atrocities could erode trust in one of India's most respected institutions within hours.

ii. Hashtag Engineering and Trend Hijacking
Bot networks and troll farms artificially inflate hashtags, gaming algorithms to create an illusion of consensus.

- *Risk:* During the Article 370 abrogation and CAA protests, fake accounts traced to Pakistan pushed anti-India hashtags into global trending lists.

iii. Information Saturation and Cognitive Overload
Adversaries flood the digital space with conflicting data, leaving the public overwhelmed. Confusion and apathy replace clarity.

- *Risk:* After communal riots, competing fake stories on who instigated violence often leave even credible voices disoriented.

iv. Fake News and Memetic Warfare
Simple memes and doctored infographics appeal to emotion and spread faster than fact-checks.

- *Risk:* Circulated images of desecrated temples or mosques have repeatedly triggered mob violence during festivals.

v. Diaspora-Based Narrative Seeding
Radical diaspora groups frame extremist causes as "human rights" struggles abroad, re-importing those narratives into India.

- *Risk:* Sikhs for Justice (SFJ) ran "Referendum 2020" campaigns in Canada and the UK, shaping domestic discourse in Punjab through online virality.

vi. Front NGOs and Academic Capture
Foreign-funded NGOs and think tanks cloak anti-state agendas in intellectual critique, subtly shifting global and domestic perceptions.

- *Risk:* Research funded by dubious foreign foundations has labelled counterinsurgency campaigns as systemic repression, influencing watchdog reports.

vii. Encrypted Messaging Platforms
Closed apps like Telegram, Threema, and ProtonMail enable secure mobilisation and logistics planning, beyond the reach of traditional policing.

- *Risk:* Encrypted chats were widely used to coordinate logistics during the anti-CAA protests.

viii. Foreign Media Echo Chambers
Selective stories seeded by hostile actors are amplified in global media, gaining credibility before re-entering Indian debates.

- *Risk:* Outlets like Al Jazeera and TRT World often portrayed Indian law enforcement as majoritarian crackdowns, without noting the security imperatives.

ix. Bot Armies and Automated Harassment
AI-driven bots create synthetic outrage and intimidate individuals or institutions.

- *Risk:* During India's vaccine diplomacy, bot-driven campaigns manufactured the illusion of global disapproval.

d. Real-World Illustrations

- **Pakistan's ISPR Doctrine:** The Inter-Services Public Relations wing integrates media warfare, psychological ops, and diaspora influencers to sustain anti-India narratives globally.

- **China's "Three Warfares" Strategy:** A structured doctrine blending media warfare (to dominate narratives), legal warfare (to challenge claims diplomatically), and psychological warfare (to create confusion among populations and forces).
- **Diaspora Khalistan Lobby:** Groups like SFJ fund referendums, orchestrate social media campaigns, and lobby international forums to depict Punjab as oppressed and India as authoritarian.

Conclusion

India's greatest vulnerabilities today may not lie on its borders but within its information ecosystem. Information warfare is designed to corrode trust, fragment society, and undermine the legitimacy of the state—all without firing a bullet.

Protecting sovereignty in the twenty-first century therefore requires defending not only territory but also narratives, institutions, and digital mindspace.

As Carl Miller, a cyber-warfare analyst, observes: *"The most dangerous war is the one we don't realise we're in—fought in minds, not on maps."*

The toolkit of information warfare demonstrates how espionage, ideological subversion, and digital manipulation have become central to modern internal security threats. Yet India is not unique in this struggle. Democracies and authoritarian regimes alike—from the US to Singapore, from Europe to China—have grappled with hostile narratives, cyber propaganda, and proxy activism.

Comparative global experiences offer valuable insights. They show how different systems—through legal safeguards, community resilience, counter-narrative strategies, or digital regulation—have confronted the same invisible threat. For India, learning from these models is not optional but strategic.

The next section therefore turns to global case studies and counter-models, examining how other nations have fought the silent war of influence operations—and what lessons India can draw from their successes and failures.

4.5 Case Studies / Comparative Global Models

a. Introduction

Comparative global models and landmark case studies offer two invaluable insights. First, they demonstrate how nations have adapted to the realities of hybrid, proxy, and asymmetric threats. Second, they allow India to extract best practices for strengthening its own doctrine—whether in intelligence coordination, urban counter-terror preparedness, or narrative warfare.

b. Key Case Studies

i. India–Pakistan: Kargil War (1999) and 26/11 Mumbai Attacks (2008)

Event	Key Insights
Kargil War (1999)	Pakistan's use of soldiers disguised as irregulars exemplified *hybrid warfare*—combining military engagement with the deniability of proxy actors. It exposed India's weak early-warning systems and highlighted civil–military coordination gaps. The aftermath led to the Kargil Review Committee and subsequent reforms in intelligence architecture.
26/11 Mumbai Attacks (2008)	Lashkar-e-Taiba (LeT) operatives infiltrated via the sea, using VoIP, GPS, and live handlers from Pakistan to sustain a 60-hour siege. The attacks revealed India's lack of real-time coordination and gaps in urban counter-terror capacity. Consequences

Event	Key Insights
	included the creation of the National Investigation Agency (NIA), establishment of NSG hubs, and strengthening of multi-agency coordination centres.

Both incidents underline how asymmetric and proxy warfare exploit loopholes in preparedness—forcing structural reform only after a crisis.

ii. China's United Front Strategy

China represents a model of influence operations institutionalised through the United Front Work Department, which blends state and non-state outreach. By deploying diaspora networks, Confucius Institutes, business chambers, and digital propaganda, Beijing weaponises soft power with covert strategy.

Core Objectives:

- Promote pro-China narratives abroad.
- Infiltrate policymaking circles in target states.
- Suppress dissent against the Communist Party through coordinated global pressure.

Implications for India:

- **Border Propaganda in Arunachal Pradesh**
  Beijing promotes the "South Tibet" narrative, attempting to delegitimise India's sovereignty.
- **Diaspora-Based Influence**
  Chinese-origin associations abroad are mobilised to shape discourse in neighbouring states like Nepal and Bhutan.
- **Soft Power with Subversion**
  Academic partnerships, business ties, and media narratives create an ecosystem of persuasion that complements hard power.

This model illustrates how modern statecraft fuses diplomacy, propaganda, and covert action to alter perceptions—an approach India must learn to anticipate and counter both domestically and abroad.

Conclusion

Global experiences confirm that modern threats are rarely conventional. They are hybrid, deniable, and multidimensional, operating as much in digital spaces and media narratives as in physical battlefields.

For India, resilience demands more than soldiers and statutes. It requires storytellers alongside soldiers, servers alongside spies, and strategy alongside force. National security today depends on shaping perceptions as much as defending frontiers.

As one analyst observed: *"Security is not built with soldiers alone, but with storytellers, servers, and strategy."*

The exploration of external states, non-state actors, asymmetric warfare, and influence operations highlights a common thread: the centrality of cyberspace. Whether it is Pakistan's drones and digital propaganda, China's cyber sabotage of power grids, diaspora-driven narrative engineering, or radicalisation through encrypted apps, the digital domain has emerged as the new frontline of internal security.

Unlike conventional battlefields, cyberspace is borderless, anonymous, and instantaneous. A hacker in Rawalpindi, a troll farm in Beijing, or a radicalised teenager in Kerala can have as much disruptive

impact as a conventional strike. What once required armies, camps, and logistics can now be achieved with a laptop, a VPN, and a viral message.

This reality makes cyber security not merely a technical necessity but a strategic imperative—at the intersection of national defence, economic resilience, democratic stability, and personal privacy.

The next chapter therefore turns to Cyber Security: its evolving threats, India's vulnerabilities, and the frameworks required to safeguard sovereignty in the digital age.

Chapter 5. Cyber Security

5.1 Introduction to Cyber Security

a. Introduction

In the digital age, the keyboard has become as potent as the Kalashnikov, and cyberspace has emerged as a decisive theatre of modern conflict. India's rapid digitisation—spanning governance, banking, healthcare, defence, and daily life—has enhanced efficiency and connectivity but has simultaneously multiplied vulnerabilities. With over 880 million internet users and growing dependence on digital infrastructure, the nation faces an unprecedented spectrum of threats: from ransomware and espionage to deepfakes and narrative warfare.

What makes cyber threats uniquely dangerous is their invisibility, borderless reach, and deniability. Attacks are often detected only after the damage is done; they originate from anywhere in the world, beyond conventional treaties or jurisdiction; and they enable hostile actors to mask responsibility behind anonymous proxies or mere lines of code.

As India's former National Cyber Security Coordinator, Lt. Gen. Rajesh Pant, observed:
"Today's wars are coded in silence, launched with keystrokes, and fought in shadows."

b. Major Types of Cyber Threats in India

Type of Threat	Explanation & Real-World Examples
Hacking & System Intrusions	Unauthorised access into protected networks or systems to steal, alter, or delete data. *Example:* Breach of Kudankulam Nuclear Power Plant's internal systems (2019); suspected Chinese group RedEcho targeting the Mumbai power grid (2020).
Cyber Espionage	State-sponsored infiltration to extract sensitive military, diplomatic, or strategic information. *Example:* The GhostNet operation, traced to China, which targeted Indian embassies and the Dalai Lama's communication networks.
Ransomware Attacks	Systems are encrypted or locked, with ransom (often in cryptocurrency) demanded for restoration. *Example:* AIIMS Delhi ransomware attack (2022) paralysed access to critical health data.
Data Breaches & Leaks	Exposure or illicit sale of sensitive public or private data on the surface web or dark web. *Example:* Alleged Aadhaar database leaks; CoWIN vaccination app data reportedly offered for sale on darknet forums (2023).
Phishing & Social Engineering	Fraudulent emails, messages, or websites trick users into revealing credentials or installing malware. *Example:* Widespread "sextortion scams" and fake "KYC update" alerts targeting Indian bank customers and UPI users.
Cyber Terrorism	Use of cyber tools to create panic, sabotage infrastructure, or spread extremist ideology. *Example:* ISIS-affiliated hackers defacing Indian government websites with jihadist slogans.
Disinformation & Cognitive Attacks	Use of fake news, deepfakes, and propaganda to polarise societies or manipulate democratic processes. *Example:* WhatsApp forwards inciting mob violence in Jharkhand (2018).
Zero-Day Exploits	Exploitation of unknown software vulnerabilities before developers issue security patches. *Example:* Pegasus spyware exploiting iOS zero-day flaws to surveil Indian activists and journalists.

Conclusion

For India, cybersecurity is no longer about safeguarding data alone; it is about protecting democracy, preserving developmental gains, and defending sovereignty in a hyper-connected world. The country's vulnerabilities are magnified by a combination of outdated laws, fragmented institutional capacity, and widespread digital unawareness among citizens.

Securing India's digital future will therefore demand a multi-pronged approach: strengthening deterrence and cyber diplomacy, investing in cyber forensics and awareness campaigns, and recognising that cyber threats are not merely IT problems but core national security imperatives. Analysts often warn that the next war may not begin at a physical border but with a blackout, a bank hack, or a viral video. In this context, cyber resilience is no longer optional—it is existential.

The recognition of these vulnerabilities naturally raises a critical question: how well-prepared is India to withstand and respond to such diverse cyber threats? If the previous discussion highlighted why the country is a uniquely attractive target, the next step is to examine the institutional and technological architecture that India has built to defend itself. This requires an appraisal of the agencies, laws, and frameworks that constitute the national cybersecurity infrastructure—assessing both their strengths and the gaps that still persist.

5.2 India's Cybersecurity Infrastructure

a. Introduction

India today stands at the forefront of a digital revolution. With more than 880 million internet users, record-breaking Unified Payments Interface (UPI) transactions, and an expanding drive towards AI-enabled governance, the country has woven cyberspace into the very fabric of national life. Yet this transformation has also created an expansive and porous attack surface. Cyberattacks now threaten not merely the confidentiality of data but the continuity of governance itself—targeting power grids, hospital servers, banking infrastructure, election databases, and even public trust in institutions.

In recognition of these challenges, India has built a layered cybersecurity architecture. Nodal agencies such as the Indian Computer Emergency Response Team (CERT-IN), the National Critical Information Infrastructure Protection Centre (NCIIPC), and the Indian Cyber Crime Coordination Centre (I4C) represent an ambitious attempt to combine technical monitoring, law enforcement, and strategic coordination. However, what exists on paper often falters in practice, hampered by silos, manpower shortages, and technological lag. As Lt. Gen. Rajesh Pant, former National Cybersecurity Coordinator, warned: *"We are connecting everything—but protecting very little."* Without synergy, real-time intelligence sharing, and legislative modernisation, India's defences risk becoming a digital Maginot Line—impressive in appearance yet vulnerable to circumvention.

b. Key Institutions and Frameworks

India's cyber defence ecosystem comprises a mix of civilian, military, and technical bodies.

- **Indian Computer Emergency Response Team (CERT-IN):** The nodal agency under MeitY responsible for issuing alerts, coordinating responses, conducting audits, and training. It routinely publishes advisories on ransomware variants, phishing trends, and patch requirements.
- **National Critical Information Infrastructure Protection Centre (NCIIPC):** Functioning under the NTRO, it safeguards "critical information infrastructure" in banking, power, defence, and transport. Empowered under Section 70A of the IT Act, it mandates compliance audits for vital sectors.
- **Cyber Swachhta Kendra (Botnet Cleaning Centre):** Provides public tools to detect and remove malware. Initiatives such as *AppSamvid* (application whitelisting) and *M-Kavach* (mobile security) extend cyber hygiene to the citizen level.

- **Indian Cyber Crime Coordination Centre (I4C):** Established under MHA to enhance investigative capacity through forensics, analytics, and reporting. Its National Cyber Forensic Lab and the 1930 helpline for online financial fraud victims are key initiatives.
- **Defence Cyber Agency (DCA):** Operating under the Integrated Defence Staff, it handles both defensive and offensive military cyber operations, securing armed forces' networks and planning cyber warfare.
- **National Cyber Security Coordinator (NCSC):** Based in the PMO, it oversees strategic-level policy and represents India in international cyber dialogues.
- **National Cyber Security Policy, 2013 (under revision):** India's overarching framework for cyber resilience, skill-building, and public–private participation. A much-needed updated version is expected soon to reflect AI, IoT, and blockchain challenges.

c. Key Gaps and Challenges

- **Fragmented Institutional Architecture**
  Cyber responsibilities are scattered across MeitY, NTRO, MHA, and MoD, creating silos. CERT-IN and law enforcement agencies, for instance, have struggled to coordinate effectively on ransomware investigations.
- **Slow Threat Attribution and Response**
  Even when attacks are traced to foreign servers, proving state involvement remains diplomatically difficult, delaying counter-measures.
- **Critical Infrastructure Vulnerability**
  Banking, energy, and healthcare remain under-protected. Red teaming and penetration testing are exceptions rather than norms, raising the risk of catastrophic "Black Swan" events.
- **Acute Manpower Deficit**
  India faces a shortfall of over one million cybersecurity professionals. Police cyber cells and research labs lack expertise in OSINT, malware analysis, blockchain tracing, and drone forensics.
- **Outdated Legal Frameworks**
  The IT Act, 2000—framed in a pre-smartphone era—does not adequately address ransomware, deepfakes, or IoT vulnerabilities. Even the Digital Personal Data Protection Act, 2023 leaves gaps in cross-border enforcement.
- **Civil–Military–Private Disconnect**
  The DCA rarely coordinates with CERT-IN or I4C outside crisis situations, while private companies hesitate to share breach data due to unclear liability safeguards.
- **Weak Real-Time Monitoring**
  India lacks a unified cyber command or real-time threat fusion centre across civilian, defence, and private networks, leaving responses largely reactive.
- **Global Non-Alignment**
  India has not signed the Budapest Convention on Cybercrime, limiting access to cross-border evidence. MLATs remain cumbersome and under-utilised.

Conclusion

India's cybersecurity landscape must evolve from reactive containment to resilient anticipation. The new frontier of conflict includes not just borders but algorithms, server farms, and synthetic narratives. Securing this domain requires a recalibration of both policy and practice: a centralised national cyber command integrating civil, military, and private actors; real-time intelligence fusion centres; forward-looking legislation on AI, IoT, and blockchain; and a massive push for skill development in ethical hacking and cyber forensics.

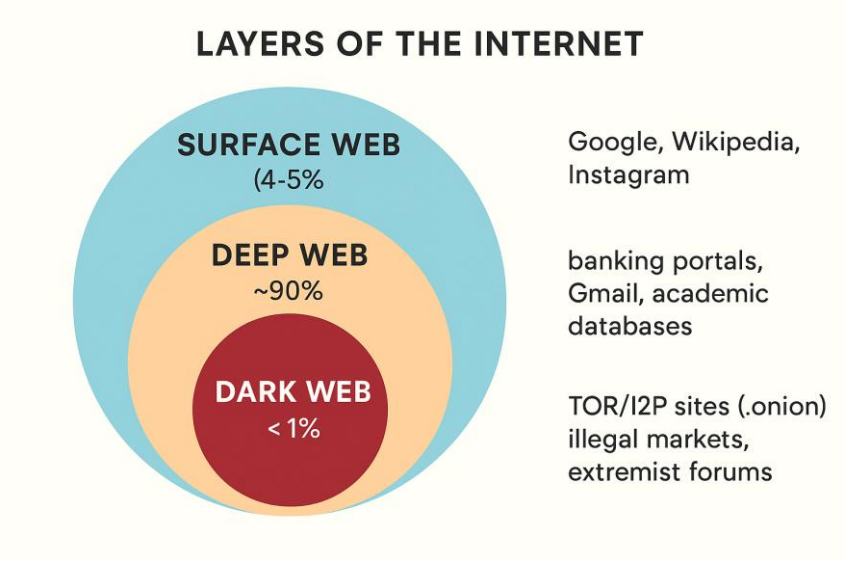
Ultimately, cybersecurity is about safeguarding democracy, sovereignty, and citizen dignity in a hyper-connected world. India's rise as a digital power will depend not merely on the scale of its digital revolution but on the resilience of the shield that protects it.

If India's formal cybersecurity infrastructure represents the visible shield, then the dark web and anonymous networks form the shadow battlefield where many of these threats originate. Beyond the regulated surface web lies an ecosystem of TOR markets, encrypted forums, and clandestine communication channels. Here, cybercriminals trade stolen data, extremists spread propaganda, and hostile actors probe India's resilience. Understanding this domain is therefore essential—not only to grasp the full spectrum of risks but also to appreciate the limits of state control in an era of decentralised, anonymous networks.

5.3 The Dark Web, TOR, and Anonymous Networks

a. Introduction

The internet, often celebrated as a tool of empowerment and connectivity, conceals layers far deeper than what most users encounter. The visible or *surface web*, comprising search engines, social media, and news sites, accounts for barely five percent of the whole. Beneath lies the *deep web*—databases, academic repositories, and password-protected portals—and further still, the *dark web*: a realm designed for anonymity and deliberate concealment.



Accessible only through anonymising software such as The Onion Router (TOR) or the Invisible Internet Project (I2P), the dark web embodies a paradox. It serves as a sanctuary for dissidents and journalists evading censorship, but equally as a marketplace for narcotics, arms, stolen data, child sexual abuse material (CSAM), terrorist propaganda, and ransomware.

For India, the risks are magnified by its massive pool of first-generation digital users, evolving crypto-regulation, and limited cyber forensic capacity. Extremist organisations, drug cartels, and cyber mercenaries exploit this shadow ecosystem to bypass borders, evade laws, and erode state authority. As the Cyber Peace Foundation notes: *"The dark web is the digital equivalent of international waters—lawless, anonymous, and perilously accessible."*

Understanding this hidden layer is therefore not optional—it is a national security imperative.

b. Key Concepts Explained

- **Deep Web:** Non-indexed content such as personal emails, banking portals, and institutional databases; not illegal in itself.
- **Dark Web:** A subset of the deep web accessible only through anonymising browsers. Hosts "hidden services" with untraceable addresses, often used for illicit activity.
- **TOR Network (The Onion Router):** Routes traffic through multiple volunteer-operated nodes to mask identity. Offers anonymity but also shields criminals.
- **Anonymous Networks (I2P, Freenet):** Peer-to-peer, censorship-resistant ecosystems, frequently used for black markets and extremist forums.

c. Why the Dark Web Threatens India's Internal Security

- **Illegal Weapons and Narcotics:** Encrypted platforms facilitate the trade of arms, drugs, and explosives, delivered through covert courier chains. Narcotics linked to darknet sales have already been traced to Indian crypto wallets.
- **Sale of Hacked Data:** Aadhaar details, CoWIN vaccination records, and banking credentials frequently surface on darknet markets, auctioned to global buyers.
- **Terrorism and Radicalisation:** Extremist groups circulate bomb-making guides, propaganda, and recruitment videos through dark web forums. ISIS and Al-Qaeda have used TOR-based channels for indoctrination.
- **Child Sexual Abuse Material (CSAM):** India ranks among the top global consumers of CSAM, much of which circulates through dark web networks.
- **Crypto Laundering and Ransomware:** Ransomware syndicates demand cryptocurrency payments—often in privacy coins like Monero—making tracking difficult.
- **Disinformation Campaigns:** Encrypted forums incubate hate propaganda and "toolkits," which later spill over into mainstream platforms, destabilising social harmony.

d. Challenges in Policing the Dark Web

- **Encryption and Anonymity:** TOR and I2P route traffic through multiple layers of encryption, rendering user identification near-impossible without privacy breaches.
- **Jurisdictional Barriers:** Servers are often hosted abroad; MLATs are cumbersome and cooperation from countries like China remains unlikely.
- **Forensic Deficits:** Most agencies lack crawler software, blockchain analysts, and skilled forensic labs to track darknet activity.
- **Identity Obfuscation:** Aliases, burner emails, and anonymous wallets frustrate attribution.
- **Cryptocurrency Payments:** Transactions through Monero or layered Bitcoin wallets complicate forensic trails; India lags in advanced crypto-tracing.
- **Lack of Real-Time Monitoring:** Unlike the U.S. or Israel, India lacks a continuous darknet surveillance command.
- **Legal–Ethical Dilemmas:** Honeypots or state malware raise constitutional questions in light of the *Puttaswamy* privacy judgment.
- **Under-Reporting:** Crimes like sextortion or identity theft often go unreported due to stigma or fear, skewing data and policy responses.

Conclusion

The dark web has created an arena of conflict that recognises neither geography nor conventional hierarchies. Its weapons are anonymity, encryption, and access. For India, this has transformed internal security into a struggle waged as much in digital shadows as on the ground.

Countering this invisible adversary requires investment in AI-driven dark web intelligence platforms, advanced crypto-tracing infrastructure, and expanded forensic training at both central and state levels. Legal frameworks must strike a delicate balance: enabling calibrated surveillance while upholding constitutional safeguards. As one analyst warned: *"Tomorrow's terrorists will not cross borders—they will cross firewalls."*

If the dark web represents today's hidden battlefield, the next wave of cyber conflict is already unfolding in plain sight. Artificial intelligence is being weaponised for automated hacking and disinformation, deepfakes erode the line between truth and fiction, and quantum computing threatens the very foundations of encryption. These emerging technologies signal that India's challenge lies not just in confronting current dangers but in anticipating a far more disruptive cyber future.

5.4 Emerging Domains: AI in Cyberattacks, Deepfakes, and Quantum Threats

a. Introduction

Cybersecurity is rapidly moving beyond the era of passwords and firewalls. The threats of tomorrow are intelligent, adaptive, and deceptive—powered by Artificial Intelligence (AI), deepfakes, and quantum computing. These are not incremental changes but disruptive enablers that democratise power, giving even small groups or lone individuals the capacity to cause disproportionate harm.

For India—where digital penetration is deep but awareness, law, and regulation often lag—these emerging domains create an especially volatile mix. The battles of the future will not be fought only with malware; they will be waged with algorithms that manipulate perception, machines that learn to evade detection, and quantum systems capable of rendering current encryption obsolete. As one analyst warned: *"The most dangerous cyberattacks of tomorrow won't come with a bang—but with a whisper generated by an algorithm."*

b. Key Emerging Threat Vectors

- **AI-Powered Cyberattacks:** AI automates phishing, scans networks for vulnerabilities, and deploys adaptive malware that alters its signature in real time. Indian banks and defence networks have already reported spear-phishing attempts generated by AI, virtually indistinguishable from genuine communication.
- **Deepfakes and Synthetic Media:** AI-generated video and audio can convincingly mimic leaders or institutions, weaponised to defame, manipulate public opinion, or blackmail. A deepfake of an army officer or communal hate content can trigger unrest before verification is possible.
- **Cognitive Warfare Tools:** Predictive algorithms allow micro-targeting of citizens using data scraped from social media. During elections, AI-driven bots can amplify divisive content, subtly steering voter sentiment and fuelling polarisation.
- **Quantum Computing (Future Threat):** Once mature, quantum systems will be capable of breaking encryption standards such as RSA and AES. This threatens defence communications, financial systems, and Aadhaar-linked databases—potentially rendering existing safeguards obsolete overnight.

- **Generative AI and Chatbot Misuse:** Large language models can draft convincing phishing emails, generate malicious code, or create fabricated narratives. "AI-powered cybercrime manuals" and malware prototypes are already circulating on darknet forums.

c. Why Emerging Technologies Are Hard to Regulate

- **Global and Decentralised Access:** Many AI or deepfake tools are open-source and globally distributed. Even if restricted in India, they remain accessible through VPNs, mirror sites, and repositories such as GitHub.
- **Absence of Tailored Legal Frameworks:** India lacks specific provisions addressing synthetic media, quantum vulnerabilities, or AI misuse. Reliance on the Information Technology Act, 2000—a pre-smartphone era law—creates a wide regulatory gap.
- **Attribution and Accountability Challenges:** AI-generated content blurs responsibility. If a chatbot generates hate speech or malicious code, should liability rest with the user, the developer, or the platform?
- **Indistinguishability of Synthetic Content:** As deepfakes grow more realistic, even forensic experts struggle to distinguish fake from authentic. This complicates takedown orders, criminal investigation, and public awareness.
- **Dual-Use Dilemma:** Technologies that revolutionise healthcare or finance can equally be weaponised. AI aids in cancer detection but also in cyber intrusions; quantum secures transactions yet threatens global encryption.
- **State Use of Emerging Tools:** Governments—including India—employ AI-driven surveillance and predictive policing. Oversight becomes politically sensitive when the state itself is a user of opaque, high-risk tools.
- **Shortage of Skilled Regulators:** Regulators, judges, and bureaucrats often lack technical expertise to audit AI systems, evaluate quantum risk, or detect deepfakes. Unlike the EU's AI Act or U.S. oversight bodies, India has no specialised authority empowered to certify or enforce compliance.

Conclusion

The true danger of emerging technologies lies less in their existence and more in the velocity of their evolution, which far outpaces society's capacity to regulate, understand, or defend against them. AI-driven misinformation, deepfake propaganda, and quantum-enabled decryption threaten not only infrastructure but also the very integrity of truth, trust, and sovereignty.

India's response must be anticipatory rather than reactive. This requires:

- A national framework for AI ethics and cyber-risk governance.
- Investment in quantum-resilient encryption and deepfake detection technologies.
- Establishment of cross-domain regulatory bodies combining technical, legal, and ethical expertise.
- Training for the judiciary, regulators, and civil servants in technological literacy.
- Mandatory audits and watermarking of AI-generated outputs.

As one expert cautions: *"The enemy of the future is not a soldier or a spy—it is a line of code that knows you better than you know yourself."* India must therefore secure not only its networks but also the dignity of its citizens and the resilience of democratic discourse.

The disruptive potential of AI, deepfakes, and quantum computing highlights a critical truth: technological innovation is outpacing the laws meant to govern it. No matter how advanced India's cybersecurity infrastructure becomes, its effectiveness will ultimately depend on the legal and regulatory frameworks that define the boundaries of action. Having explored the threats shaping the cyber domain, the next section turns to India's legal and regulatory landscape—examining how the IT Act, data protection regimes, and institutional oversight attempt to keep pace with this fast-evolving battlefield.

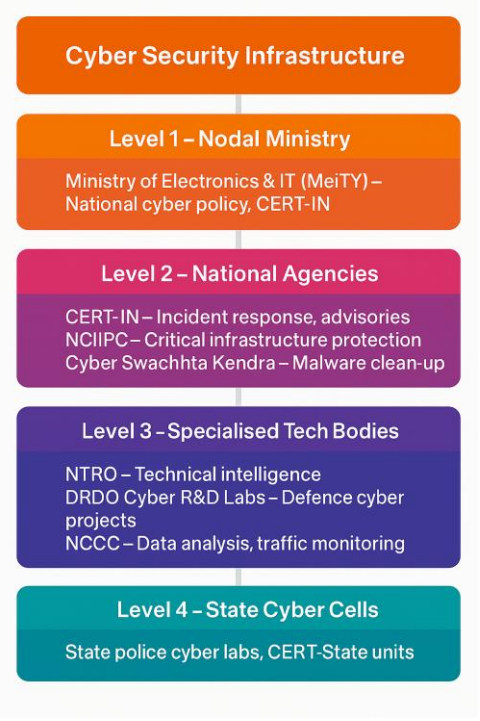
5.5 Legal and Regulatory Framework for Cybersecurity in India

a. Introduction

India's headlong rush into the digital age has far outpaced the legal scaffolding meant to secure it. While platforms, threats, and vulnerabilities have multiplied—from AI-powered malware to cryptocurrency laundering—the country's laws remain fragmented, outdated, and largely reactive. The Information Technology Act of 2000 continues to be the primary statute, despite having been conceived in a pre-social media era, while newer instruments such as the Digital Personal Data Protection Act of 2023 offer partial safeguards but stop short of creating a comprehensive framework.

At the heart of the challenge lies a double dilemma. On the one hand, the tension between security and privacy has intensified, with surveillance powers expanding in ways often lacking judicial oversight. On the other, the balance between innovation and regulation remains elusive, as policymakers hesitate to restrain technologies that drive economic growth, even when they introduce grave security risks. In an era where "data is the new oil" and algorithms evolve faster than courts, India's legal response must shift from patchwork fixes to anticipatory, rights-respecting governance. As one commentator aptly put it: *"A nation that codes faster than it legislates is a nation whose digital future is unsecured."*

b. Key Legal Instruments in India

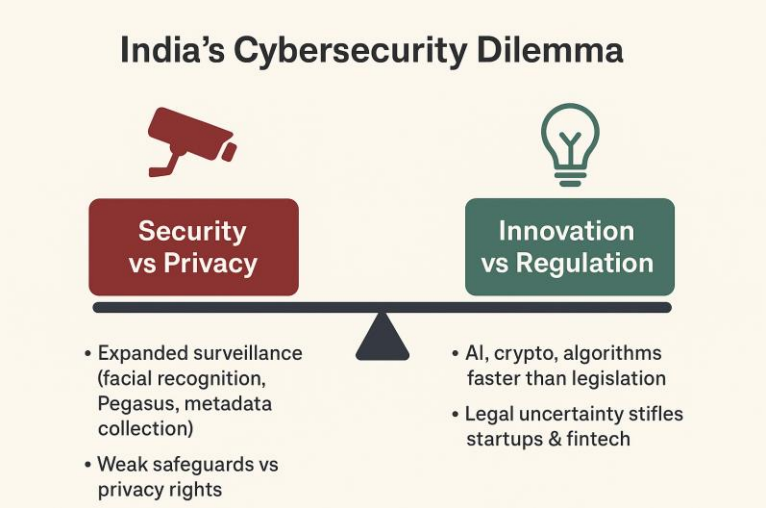


- **Information Technology Act, 2000 (IT Act):** The foundational law covering offences such as hacking, data theft, cyber terrorism, and online obscenity. Its provisions, however, are rooted in an early-internet era and do not adequately address AI intrusions, crypto-financed crime, or disinformation warfare.
- **Digital Personal Data Protection Act, 2023 (DPDP):** India's first dedicated privacy law, based on principles of consent and individual data rights (access, correction, erasure). It establishes a Data Protection Board, but critics highlight its broad exemptions for government agencies and its reliance on civil, not criminal, penalties.
- **Puttaswamy Judgment (2017):** The Supreme Court's recognition of the Right to Privacy as a fundamental right under Article 21. By laying down the principles of legality, necessity, and proportionality, it provides a constitutional yardstick for evaluating state surveillance and data protection.
- **Bharatiya Nyaya Sanhita (BNS), 2023:** The updated penal code incorporates offences like online stalking, electronic impersonation, and digital cheating. Yet it does not grapple with cross-border attribution, blockchain forensics, or the evidentiary complexities of cybercrime.
- **National Cyber Security Policy, 2013 (under revision):** India's first cyber strategy emphasised critical infrastructure protection, capacity building, and PPPs. A more ambitious National Cybersecurity Strategy (drafted in 2021) remains pending, leaving India without an updated doctrine for the AI–quantum era.

c. Key Gaps and Concerns

- **Absence of a Unified Cybersecurity Law:** Provisions are scattered across the IT Act, BNS, DPDP, and executive orders, creating overlaps and enforcement blind spots. India lacks an umbrella statute integrating infrastructure defence, cross-border evidence frameworks, and deterrent penalties.

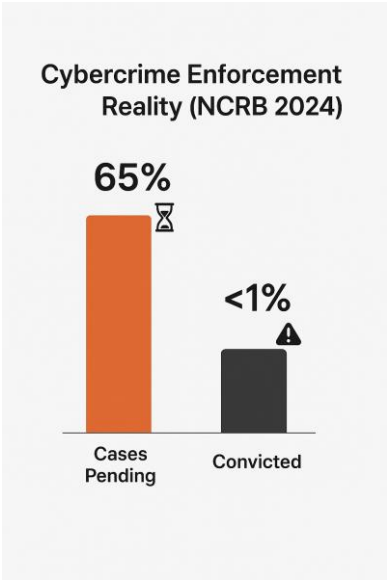
- **Surveillance Without Oversight:** Tools like facial recognition systems and spyware operate under broad executive mandates. Without parliamentary or judicial checks, they risk violating the Puttaswamy test of proportionality.
- **Data Protection vs National Security:** The DPDP Act exempts government agencies under vague grounds like "public order" and "sovereignty," raising fears of unchecked mass surveillance.



- **Weak Enforcement:** Conviction rates for cybercrime remain below 1%, due to poor digital evidence handling, weak forensic capacity, and procedural delays. Cases linger for years, eroding deterrence.
- **Legal Vacuum Around Emerging Technologies:** Existing laws are silent on deepfakes, generative AI abuse, ransomware funded by crypto, or algorithmic bias. India lacks statutory mechanisms for AI audits or liability attribution.
- **Intermediary and Developer Liability Gaps:** Social media platforms, data brokers, and AI developers escape accountability for harms such as fake news or manipulative design. Unlike the EU Digital Services Act, India has no clear liability chain for intermediaries.
- **Judicial and Enforcement Deficit:** Courts, prosecutors, and police lack training in blockchain analysis, deepfake forensics, or AI-related evidence. This capacity gap fuels delays and dependence on foreign expertise.
- **Reactive Policy Landscape:** Most cyber policies are ad hoc, relying on advisories rather than binding doctrines. The National Cybersecurity Strategy remains unadopted, leaving India without a future-facing legal blueprint.

Conclusion

India's current cyber legal framework is ill-suited for the speed, scale, and sophistication of modern digital threats. What exists today is a patchwork of legacy laws, sectoral gaps, and unenforced policies—far from the holistic Cyber Law 2.0 that the country requires.



Such a paradigm shift must include:

- An umbrella cybersecurity law integrating all aspects of digital risk.
- Explicit accountability for intermediaries and AI developers.
- Independent oversight of surveillance powers to uphold constitutional principles.
- Judicial and police capacity-building in cyber forensics and AI evidence.
- A forward-looking national strategy addressing AI, quantum, and IoT vulnerabilities.

As of 2024, over 65% of cybercrime cases in India remain under investigation beyond one year, with conviction rates negligible across states. In cyberspace, delay itself is vulnerability. The lesson is clear: *"Laws must be coded as swiftly as the threats they intend to tame."*

While laws and regulations provide the foundation for managing cyber risks within national borders, cyber conflict today transcends them. Cyberattacks are no longer limited to isolated crimes or corporate breaches—they are increasingly deployed as instruments of statecraft, coercion, and war. For India, the challenge lies not only in protecting its domestic digital ecosystem but also in building sovereign cyber capabilities in a world where hostile nations weaponise code as effectively as conventional arms.

The next section therefore turns to Cyber Warfare—examining its evolving nature, India's vulnerabilities, and the imperatives of securing national sovereignty in this contested domain.

5.6 Cyber Warfare

a. Introduction

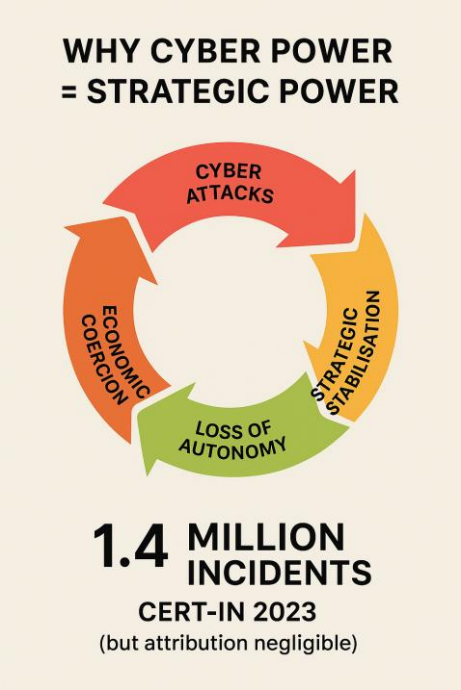
Cyber warfare represents one of the newest—and most insidious—forms of conflict in the twenty-first century. Nation-states and their proxies increasingly deploy digital weapons to compromise, disrupt, or manipulate the critical information infrastructure of rivals, often without firing a single shot. Unlike conventional wars, these contests are silent, borderless, and continuous, existing in the grey zone between peace and open conflict.

The objectives of cyber warfare are rarely territorial. Instead, they are designed to paralyse economies, disrupt governance, steal information, spread disinformation, and erode public confidence. Cyber operations often form part of a broader hybrid conflict strategy that blends information warfare, economic sabotage, and psychological operations. As one strategist aptly observed:

"The twenty-first century's most dangerous battlefield is invisible, silent, and borderless—it lies within code, cables, and clouds."

b. Key Features of Cyber Warfare

- **No Formal Declaration:** Cyber operations occur below the threshold of conventional war, with no declarations or visible mobilisation.
- **Remote Execution:** Attacks can be launched remotely across borders with minimal physical risk to the attacker.
- **Targeted Disruption:** The aim is not outright destruction but the disabling of systems, theft of data, or erosion of trust.
- **Difficult Attribution:** Perpetrators hide behind multiple proxies, false trails, and spoofed infrastructure, making attribution slow and inconclusive.
- **Psychological Impact:** Beyond technical damage, cyberattacks are intended to sow panic, weaken morale, and delegitimise institutions.



c. India's Strategic Threat Perception

India finds itself increasingly targeted by both hostile states and non-state actors, with cyber operations threatening critical infrastructure, strategic assets, and societal cohesion.

- **China:** Linked groups such as RedEcho were suspected in the 2020 cyberattack on Mumbai's power grid. Chinese operators have targeted the Tibetan diaspora, the office of the Sikyong, and may exploit inexpensive Chinese devices and apps to harvest data.
- **Pakistan:** ISI-backed groups such as APT36 run phishing campaigns, deface government websites, and launch propaganda drives during crises. Fake job portals targeting Indian armed forces illustrate the blending of espionage and social engineering.
- **Non-State Actors:** Ransomware groups like LockBit, REvil, and DarkSide exploit vulnerabilities across Indian systems, while darknet forums sell sensitive data including Aadhaar, CoWIN, and UPI-linked credentials. Cryptocurrency serves as the preferred vehicle for laundering and extortion.

d. Cyber Warfare Targets in India

- **Health Sector:** The AIIMS ransomware attack (2022) paralysed medical services for weeks, while breaches of the CoWIN vaccination portal exposed sensitive citizen data.
- **Power and Energy:** The RedEcho operation suspected in the 2020 Mumbai blackout demonstrated the fragility of urban grids. Earlier, the Kudankulam Nuclear Power Plant (2019) also reported breaches.
- **Defence Establishments:** Repeated attempts have been made to compromise DRDO servers, while phishing emails disguised as foreign job offers have targeted serving army personnel.
- **Banking and Finance:** Indian banks face phishing kits, carding fraud, fraudulent UPI apps, and laundering through crypto channels—undermining trust in digital financial systems.
- **Police and Intelligence:** Databases such as CCTNS have been attacked, while the Pegasus spyware revelations highlighted vulnerabilities at the highest levels of governance. Fake social media accounts impersonating police departments have further eroded credibility.

Conclusion

Cyber warfare is no longer a hypothetical threat—it is already reshaping how power is exercised, sovereignty contested, and wars fought. India's adversaries have weaponised cyberspace to undermine confidence, disable critical services, and disrupt governance, all without crossing physical borders.

Strategic autonomy in the digital age demands that India act decisively. A comprehensive national cyber warfare doctrine must be articulated, underpinned by:

- Indigenous defence capabilities in AI-driven monitoring and cyber-forensics.
- Robust deterrence through credible offensive capabilities.
- Integrated response mechanisms linking civil, military, and private infrastructure.

The scale of the challenge is immense. CERT-IN reported over 1.5 million cyber incidents in 2023, yet attribution remains elusive, with only a fraction conclusively traced or prosecuted. Tanks and missiles remain vital, but in the twenty-first century, sovereignty will also depend on firewalls, resilient code, and credible cyber deterrence.

In the digital battlefield, cyber power is strategic power.

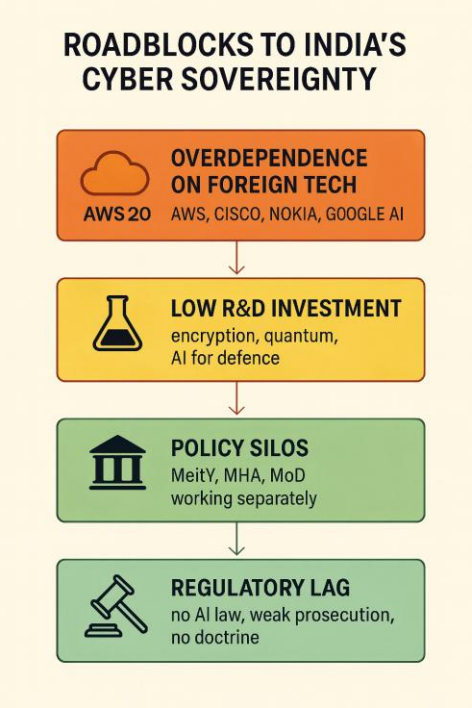
5.7 Strategic Autonomy in the Cyber Domain

a. Introduction

In the twenty-first century, cyber sovereignty is no longer a peripheral concern—it has become the foundation of national security and statecraft. Securing cyberspace is not merely about building digital firewalls; it is about ensuring that a nation retains the freedom to control its data flows, safeguard critical infrastructure, and operate its digital economy without undue dependence on foreign platforms or geopolitical alignments.

As algorithms increasingly dictate economic growth, military strength, and societal cohesion, the autonomy to shape and secure one's cyber ecosystem functions as a form of armour. India's position, however, is precarious. More than three-fourths of its cloud data is hosted on foreign servers—primarily with U.S.-based providers like Amazon Web Services, Google Cloud, and Microsoft Azure. Similarly, nearly 90 percent of its smartphone baseband chips are imported. Dependencies that seem benign in times of stability can transform into strategic vulnerabilities during geopolitical tensions, exposing India's digital backbone to coercion or surveillance.

As one expert aptly put it: *"In cyberspace, autonomy is not an option—it is armour."*



b. Pillars of Cyber Strategic Autonomy

India's digital sovereignty rests on several interdependent pillars:

- **Indigenous Technology Ecosystem:** Reducing dependence on imported routers, chips, operating systems, and cloud services is crucial. While Production-Linked Incentive (PLI) schemes for semiconductors and initiatives like OpenForge for government software have begun this journey, investments in indigenous encryption tools and secure operating systems remain inadequate.
- **Sovereign Infrastructure:** Critical national data must reside within servers governed by Indian law. Policies such as the MeghRaj National Cloud mark progress, but private platforms continue to host the majority of Indian data offshore.
- **Data Localisation:** Sensitive financial and health data must be stored within India's borders. The Reserve Bank of India has mandated localisation for payment data, yet the Digital Personal Data Protection Act (2023) allows exemptions for cross-border transfers, leaving significant gaps.
- **Cyber Talent and R&D:** Building a cadre of ethical hackers, forensic analysts, and malware researchers is vital. However, India faces a shortage of over one million professionals, with university curricula lagging behind industry requirements.
- **Cyber Diplomacy and Norms:** India must shape international cyber norms that align with its values of privacy and equity. While active in the UN Group of Governmental Experts and the Open-Ended Working Group, India remains outside the Budapest Convention on Cybercrime, limiting its ability to pursue transnational cooperation.

c. Challenges to Achieving Cyber Sovereignty

Despite progress, India's pursuit of cyber autonomy faces serious hurdles:

- **Overdependence on Foreign Technology:** Reliance on foreign-owned cloud platforms, telecom infrastructure, and proprietary software creates systemic vulnerabilities.
- **Low Domestic R&D Investment:** Funding in areas such as quantum-safe networks, AI-driven cyber defence, and indigenous encryption remains insufficient.

- **Policy Silos and Bureaucratic Fragmentation:** Cyber responsibilities are scattered across MeitY, MHA, MoD, CERT-IN, and other entities, with no unified national cyber command.
- **Regulatory Lag:** Outdated legal frameworks, weak enforcement of cybercrime laws, and the absence of a comprehensive national cyber doctrine leave India ill-prepared for fast-evolving threats.

Conclusion

India's vision of Atmanirbhar Bharat cannot remain confined to industrial production or defence hardware; it must decisively extend into the digital realm. True cyber sovereignty demands:

- Development of indigenous and secure technology infrastructure.
- Enforceable data sovereignty through localisation and encryption standards.
- A centralised cyber command for unified defence.
- Proactive engagement in shaping global AI and quantum security norms.

The stakes are stark. According to NASSCOM, India will require over 1 million cybersecurity professionals by 2030, yet current educational output meets barely five percent of this demand. The gap is not just numerical—it is strategic.

Future conflicts may be fought less with missiles and tanks and more with malware, misinformation, and microchips. To preserve autonomy and secure its place in the global order, digital self-reliance must become as urgent a priority as border defence.

Yet, cyberspace by its very nature cannot be secured in isolation. Attacks often originate across borders, routed through multiple jurisdictions, and amplified by transnational networks. No nation, however powerful, can address the challenges of attribution, enforcement, or deterrence alone. This makes international cooperation and global cyber norms indispensable. For India, the task ahead is twofold: to safeguard its interests within existing frameworks while also shaping new rules of responsible state behaviour in cyberspace—rules that balance security, privacy, and equity.

5.8 International Cooperation and Cyber Norms

a. Introduction

Cyber threats are inherently transnational. A single malware strand can be coded in one jurisdiction, launched from another, routed through multiple servers worldwide, and strike victims thousands of miles away. No nation—however advanced—can manage such borderless dangers alone. This reality makes international cooperation and harmonised cyber norms indispensable.

For India, the objectives are clear: track cross-border cybercriminals, coordinate global responses to cyberterrorism, prevent misuse of cyberspace by hostile state and non-state actors, and promote a rules-based global cyber order that balances sovereignty with openness. As one analyst remarked: *"Just as we need rules for war, we now need rules for Wi-Fi."*

b. India's Multilateral Engagements

India has steadily expanded its role in shaping international cyber governance:

- **United Nations Group of Governmental Experts (UNGGE):** India participates in drafting voluntary norms emphasising state responsibility, due diligence in preventing cyberattacks, and the protection of civilian infrastructure.
- **UN Open-Ended Working Group (OEWG):** India supports a multistakeholder approach, stressing capacity-building for the Global South to ensure digital equity.
- **Shanghai Cooperation Organisation (SCO):** Engagements focus on cyberterrorism, online content regulation, and technology localisation. However, India must balance SCO's restrictive preferences with its own commitment to an open internet.
- **G20 and BRICS:** As G20 president, India spotlighted secure digital infrastructure, cross-border data governance, and ethical AI use. Within BRICS, it has pushed initiatives for ransomware tracking and secure fintech ecosystems.
- **INTERPOL:** Indian agencies actively join joint investigations, darknet financial tracking, and monitoring of child sexual abuse material. The I-CAN initiative demonstrates the value of collective intelligence-sharing.

c. Key Global Instruments and Treaties

India's engagement with cyber norms also intersects with major global instruments:

- **Budapest Convention (2001):** The first binding treaty on cybercrime, enabling harmonised laws, evidence-sharing, and mutual legal assistance. India has refused to sign, citing sovereignty concerns and insisting on UN-led inclusive processes.
- **Tallinn Manual:** A non-binding NATO-backed guide interpreting international law in cyberspace, including norms of self-defence and state responsibility. While influential, India remains cautious given its Western orientation.
- **Global Forum on Cyber Expertise (GFCE):** India participates to share technical expertise, capacity-building initiatives, and best practices for responsible state behaviour.

d. Bilateral Cooperation

Alongside multilateral forums, India pursues targeted partnerships with key cyber powers:

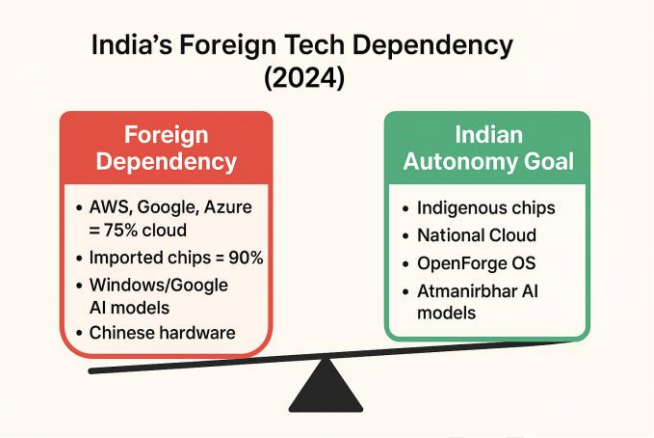
- **United States:** Framework Agreement (2016), Indo–US Cyber Dialogue, and a Joint Working Group on Counterterrorism and Cybersecurity—covering threat intelligence, capacity-building, and law enforcement.
- **Israel:** A trusted defence cybersecurity partner, collaborating on CERT-to-CERT coordination, joint R&D, and infrastructure security.
- **Japan:** Since 2018, regular cyber dialogues have focused on norms in the Indo-Pacific and securing digital supply chains.
- **France:** The Indo-French Roadmap on Cybersecurity and Digital Technology (2022) strengthens cooperation in cloud, 5G, and critical infrastructure.
- **United Kingdom:** Focuses on cybercrime investigation, police training, and securing frameworks for digital trade.

e. India's Challenges in Global Cyber Cooperation

Despite being the world's second-largest internet hub, India has yet to assert itself as a decisive voice in global cyber governance. Its cyber diplomacy often remains cautious, sovereignty-centric, and reactive—limiting its ability to shape emerging rules of the digital order. Several systemic and strategic obstacles continue to constrain its influence:

- **Sovereignty versus Surveillance Dilemma**

- India has resisted joining treaties such as the Budapest Convention, fearing erosion of sovereign control over domestic data.
- Preference is given to bilateral Mutual Legal Assistance Treaties (MLATs) and direct CERT-to-CERT collaboration.
- While sovereignty-first postures safeguard autonomy, they also marginalise India in global norm-setting processes.



- **Asymmetric Capacity in Enforcement**
  - Despite cooperation frameworks, India's enforcement capacities remain uneven.
  - Tier-2 and tier-3 cities often lack cyber forensic labs, trained personnel, or rapid response capacity.
  - This weakens India's ability to provide admissible evidence or meaningfully contribute to joint international operations.
- **Domestic Policy Fragmentation**
  - Cyber law and diplomacy are spread across multiple ministries—MeitY, MHA, MoD, NTRO, and CERT-IN—without a central coordinating authority.
  - Absence of a unified cyber doctrine weakens India's representation in forums such as the UN or G20, where coherent national positions are critical.
- **Complex Legal Environment**
  - India's emphasis on data localisation often clashes with frameworks such as the EU's free data flow with safeguards.
  - Such divergences complicate joint investigations, evidence sharing, and global interoperability of enforcement standards.
- **Trust Deficit with Global Platforms**
  - India's demands for intermediary liability, encryption backdoors, and strict takedown mechanisms have created friction with foreign tech giants, especially US-based firms.
  - While protecting sovereignty, this adversarial stance often obstructs broader alignment with global practices.
- **Underrepresentation in Cyber Norm-Making**
  - Global bodies remain dominated by Western democracies, while China and Russia advance state-controlled cyberspace models.
  - India, despite its digital size, lacks a robust cadre of cyber diplomats, think tanks, and academic programmes to influence global agenda-setting consistently.
- **Weak Capacity for Attribution and Retaliation**
  - Unlike the US or Israel, India rarely attributes cyberattacks to specific adversaries.
  - This cautious approach diminishes deterrence credibility and undermines its bargaining power in cyber diplomacy.

f. Way Forward for Strengthening India's Global Cyber Posture

For India to transition from a sovereignty-conscious participant to a norm-shaping leader, a recalibration of strategy is essential:

- **Finalise a National Cybersecurity Strategy**

- The long-pending draft must be adopted to harmonise roles across ministries, establish offensive and defensive cyber commands, and articulate a doctrine of cyber deterrence.

- **Reform Domestic Laws for Global Alignment**
  - Outdated statutes such as the IT Act (2000) must be replaced with laws integrating AI, cryptocurrency, and algorithmic transparency.
  - Interoperability with global frameworks like the GDPR and FATF norms is crucial.
- **Calibrated Participation in Treaties**
  - India could explore conditional accession to the Budapest Convention with safeguard protocols.
  - Alternatively, it could lead the negotiation of a Global South–centric treaty through BRICS or G20 platforms.
- **Build a Cyber Diplomacy Cadre**
  - The MEA should nurture cyber diplomats, legal technologists, and technical standards experts.
  - Institutions modelled on the NIST (US) or ENISA (EU) could professionalise India's global engagement.
- **Capacity-Building for the Global South**
  - India can export cyber expertise, CERT infrastructure, and digital security tools to Africa, ASEAN, and SAARC.
  - This builds goodwill and reinforces India's claim to leadership.
- **Lead on Ethical Digital Norms**
  - As the world's largest democracy, India is uniquely placed to champion a free, open, and secure internet that balances surveillance with privacy.
  - Through platforms like the Quad, IPEF, and UN, India can push back against authoritarian models.
- **Strategic Use of Soft Power**
  - India can frame cyber governance in the language of rights, equity, and justice, echoing its climate diplomacy and vaccine equity approach.
  - A vision of "Cyber Swaraj", rooted in constitutional values of privacy and pluralism, could become India's distinctive global contribution.

Conclusion

India's vast digital ecosystem—spanning 850+ million users, world-leading fintech, and an expanding AI economy—makes it both a frontline target and a vital stakeholder in shaping the global cyber order. Yet a gap persists between digital scale and global influence. India ranks only 10th in the ITU's Global Cybersecurity Index (2023), far behind its potential.

The choice before India is stark. It can remain sovereignty-obsessed, defensive, and fragmented, or it can rise as a norm-shaping leader that exports democratic values of privacy, freedom, and ethical governance to the digital domain. To achieve the latter, India must harmonise domestic laws with international standards, invest in cyber diplomacy, and project a clear vision of equitable cyberspace.

As one strategist noted: *"Cyber leadership is no longer about firewalls and forensics—it is about shaping the values that will govern the global internet."*

The exploration of cybersecurity, cyber warfare, and global digital norms underscores a recurring truth: technology today is inseparable from sovereignty, legitimacy, and strategic power. Yet cyberspace is not only a battlefield of statecraft—it is also the arena where citizens interact, form opinions, and negotiate trust in institutions.

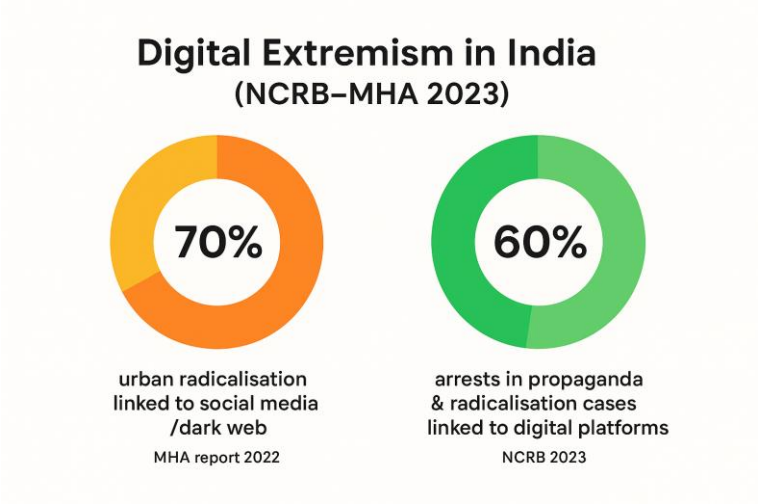
In India's experience, the same digital highways that power fintech and civic inclusion also transmit hate speech, fake news, and polarising propaganda at viral speed. Understanding this dual role is essential—not only to mitigate risks but also to harness communication networks as instruments of resilience and democratic empowerment.

The next chapter therefore turns to Communication Networks, Social Media, and Information Flows—examining how narratives, platforms, and digital ecosystems shape the security and stability of modern societies.

Chapter 6. Communication Networks, Social Media & Media Role

6.1 Uses of Communication Platforms in Threat Ecosystems

a. Introduction



In the twenty-first century, communication platforms have become far more than avenues of social interaction; they now constitute critical arenas of security contestation. From encrypted messengers to global social media networks, these platforms are deeply embedded in the operational fabric of modern threat ecosystems.

Their attractiveness stems from four defining features:

- The cloak of anonymity enabled by pseudonyms, virtual private networks (VPNs), and the dark web.
- The viral speed with which narratives can spread.
- The decentralised and jurisdiction-resistant architecture of digital space.
- The shield of end-to-end encryption that frustrates lawful surveillance.

Together, these attributes allow adversaries to evade detection, manipulate sentiment, and orchestrate violence at scale. Indian security agencies have already encountered striking instances of such misuse: the radicalisation of youth through Islamic State propaganda on Telegram; the fuelling of the 2020 Delhi riots by inflammatory WhatsApp forwards; the real-time coordination of the 2019 Pulwama terror attack through encrypted groups; and anti-state propaganda campaigns such as "Free Khalistan," engineered with offshore sponsorship.

A 2022 report by the Ministry of Home Affairs revealed that nearly seventy per cent of urban radicalisation cases in India involved exposure to social media platforms or the dark web during the early stages. This underscores their role as force multipliers for non-state actors, enabling them to operate across borders and beyond the grasp of conventional policing. As one analyst grimly observed: *"A tweet can now trigger a riot. A meme can radicalise. A livestream can coordinate crime."*

Understanding this architecture is therefore indispensable to any evolution of India's internal security doctrine, which must extend from physical surveillance to anticipatory digital foresight.

i. Recruitment and Radicalisation

Digital platforms provide fertile ground for recruitment into extremist, insurgent, or criminal groups.

- **Encrypted Messaging Applications**: Telegram, Signal, and WhatsApp allow secure one-to-one and group conversations. These are exploited to circulate ideological tracts, sermons, or videos, and to create closed grooming spaces for youth inclined towards jihadist, separatist, or left-wing extremist ideologies.
- **Gaming & Online Chat Forums**: Platforms such as Discord and Reddit increasingly target teenagers. Recruitment narratives are often framed in thrill-seeking language or identity-based appeals that resonate with vulnerable users.
- **Dark Web & Anonymous Boards**: These serve as gateways for aspiring cybercriminals and digital mercenaries. Recruitment here often involves entry-level invitations into ransomware syndicates, drug supply chains, or hacktivist groups.

ii. Propaganda and Ideological Messaging

Beyond recruitment, communication platforms are deployed to saturate the public sphere with crafted propaganda.

- **Mainstream Social Media**: YouTube, Facebook, and Instagram host videos portraying police or military operations as injustices, glorify so-called "martyrs" in Kashmir or Maoist zones, and use music, poetry, and symbolism to romanticise violence.
- **Twitter (X) and Telegram**: These act as engines of real-time propaganda—through hashtag campaigns like #FreeKhalistan or rapid wartime narrative dissemination as seen during the Ukraine and Gaza conflicts. Memes and doctored visuals make disinformation emotionally persuasive and difficult to counter swiftly.
- **Short-Form Video Platforms**: Instagram Reels and the now-banned TikTok amplify extremist reach. Their brevity and emotional pull foster "soft indoctrination," subtly priming audiences before drawing them into closed radical spaces.

iii. Coordination of Criminal or Terrorist Operations

Perhaps the most dangerous application of digital platforms lies in their operational value for violence.

- **Encrypted Messengers**: Used to transmit real-time instructions for arms movement, narcotics trafficking, or executing terrorist strikes. The Pulwama attack starkly highlighted WhatsApp's role in logistics and coordination.
- **Anonymous Handles & VPNs**: Offshore servers and pseudonymous accounts enable communications that support arms trafficking, hawala networks, and forged identity creation.
- **Geo-Targeting & Live Location**: These features allow adversaries to track police movement, coordinate flash protests, or enable lone-wolf attacks through instant "go now" directives.

Conclusion

The architecture of contemporary communication platforms—encrypted, algorithm-driven, and borderless—has fundamentally reshaped India's threat landscape. From WhatsApp coordination behind Pulwama to Khalistani reels in Punjab, evidence underscores that these platforms enable distributed and deniable ecosystems of extremism.

According to consolidated NCRB and MHA data (2023), more than sixty per cent of arrests linked to radicalisation and propaganda misuse involved digital platforms. Addressing this challenge demands a synergistic approach:

- Legal Reforms: Updating the Information Technology Act and enforcing the Digital Personal Data Protection Act.
- Technical Capabilities: Employing AI-driven open-source intelligence (OSINT) and integrated systems like NATGRID.
- Public Vigilance: Promoting digital literacy, fact-checking, and awareness against misinformation.
- Platform Accountability: Enforcing safe-harbour reforms, mandating traceability mechanisms, and ensuring compliance from tech companies.

As a senior counter-terrorism official noted: *"Digital extremism is no longer fringe—it is the frontline."*

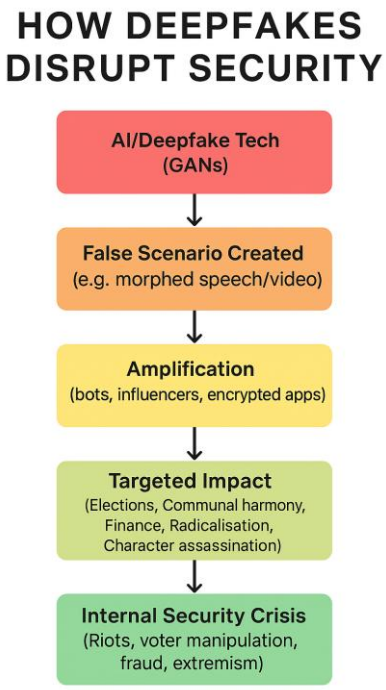
The misuse of platforms for recruitment, propaganda, and coordination demonstrates how digital highways have become enablers of extremism. Yet the threat is not confined to hidden groups or encrypted chats. Increasingly, the greater danger lies in the deliberate pollution of the information environment. Disinformation campaigns, fake news ecosystems, and synthetic media like deepfakes do not merely transmit messages—they distort truth and weaponise trust.

If encrypted platforms provide the infrastructure of extremism, disinformation and deepfakes supply the narratives that destabilise societies.
Thus, the discussion naturally shifts to the next domain: manufactured realities and factitious media factories.

6.2 Disinformation Campaigns, Deepfakes, and Fake News Factories

a. Introduction

In the twenty-first century, information is no longer merely a tool of empowerment; it has become a weapon. Disinformation campaigns, amplified by algorithms and automated bot networks, are systematically deployed to manipulate public opinion, incite unrest, delegitimise institutions, and even disrupt electoral processes.



The danger is particularly acute in India, where structural vulnerabilities magnify the threat:

- Linguistic diversity, which complicates fact-checking across multiple languages.
- Religious sensitivities, which heighten the risk of communal flare-ups.
- Low levels of digital literacy, which allow falsehoods to spread unchecked.
- High social media penetration, which provides instant reach to vast audiences.

In such a setting, a single rumour can spiral into violence within hours. Jonathan Swift's observation remains profoundly relevant: *"Falsehood flies, and truth comes limping after it."*

b. Understanding the Terminology

Clarity of terminology is essential to distinguish between varying shades of falsehood in the information ecosystem:

- **Misinformation**: False information shared without malicious intent. *Example: circulation of unverified COVID-19 cures.*
- **Disinformation**: Deliberate, coordinated falsehoods designed to mislead, manipulate, or cause harm. *Example: fabricated videos aimed at sparking communal riots.*
- **Malinformation**: Genuine information used in a misleading context. *Example: old footage of unrest circulated as a recent incident.*
- **Fake News Factories**: Organised systems that industrialise disinformation through troll farms, partisan propaganda outlets, that generate and amplify false narratives at scale.

c. Deepfakes: Artificial Intelligence as Disinformation

Deepfakes, created using machine learning techniques such as Generative Adversarial Networks (GANs), represent a new frontier of disinformation. By synthetically manipulating audio or video, they generate hyper-realistic but fabricated content capable of deceiving even trained observers.

Malicious uses include:

- **Election Interference**: Fabricated videos of candidates making inflammatory speeches can mislead voters and polarise electorates.
- **Communal Provocation**: Morphed clips of religious desecration or fabricated lynching incidents can trigger large-scale unrest.
- **Financial Fraud**: Deepfake audio mimicking a CEO has been used internationally to authorise fraudulent fund transfers.

- **Radicalisation Tool**: Fabricated atrocity videos emotionally mobilise vulnerable youth into extremist causes.
- **Character Assassination**: AI-generated intimate or compromising content has been weaponised to discredit journalists, activists, and political opponents.

d. The Disinformation Ecosystem in India

Disinformation in India operates through a complex interplay of domestic actors, foreign adversaries, and automated systems.

- **Domestic Actors**: Political IT cells, propaganda-oriented YouTube channels, and fringe groups that exploit WhatsApp forwards for communal mobilisation.
- **Foreign Actors**: Pakistan's ISI-backed bot farms, Khalistani networks in Canada and the UK, and Chinese troll factories during border tensions.
- **Automated Systems**: Bot networks and AI-driven spam engines manipulate hashtags, trend fake narratives, and spread rumours of deaths, electoral fraud, or institutional collapse.
- **Influencer Manipulation**: Paid or ideologically motivated content creators amplify false narratives via reels, Twitter threads, and podcasts, lending credibility to fabricated claims.

e. Impact on Internal Security

The consequences of disinformation are not abstract; they translate directly into security challenges:

- **Law and Order**: False messages have sparked riots, as seen in Muzaffarnagar (2013) and Bengaluru (2020).
- **Democracy**: Doctored videos, manipulated surveys, and synthetic speeches threaten electoral integrity.
- **Health Security**: During COVID-19, vaccine rumours and fake cures undermined public health drives and clogged hospital systems.
- **Radicalisation**: Emotive propaganda indoctrinated youth into Maoist, Islamist, and separatist movements.
- **Crisis Response**: During disasters, fake distress messages diverted relief resources away from genuine victims.

Disinformation and deepfake technologies have thus transformed the nature of internal security threats. They weaponise perception, erode institutional trust, destabilise democratic processes, and fragment social harmony. For a country like India, with acute societal sensitivities and vast digital penetration, the stakes are extraordinarily high.

f. Countermeasures in Place

India has begun assembling a toolkit of measures against disinformation. However, these efforts remain uneven in effectiveness and largely reactive rather than anticipatory.

- **Press Information Bureau (PIB) Fact Check Unit**: Plays a visible role in debunking viral falsehoods regarding government programmes and policies. Its limitation lies in being reactive—stepping in only after misinformation has already spread.
- **Cyber Volunteers under I4C**: Citizens are enabled to flag unlawful or suspicious content through the Indian Cyber Crime Coordination Centre. While innovative, the initiative raises concerns about potential misuse, political profiling, and chilling effects on legitimate speech.

- **Information Technology Rules (2021) and Amendments (2023)**: Mandate content originator identification, grievance redressal mechanisms, and algorithmic transparency from platforms. Critics caution that overextension may restrict free expression and erode privacy.
- **Judicial Interventions**: The Supreme Court and various PILs have underscored the need to balance free speech with security imperatives. Yet, enforcement has often been delayed, with protections arriving long after damage is done.
- **Partnerships with Social Media Firms**: Collaboration with companies like Google, Meta, and X has facilitated coordinated takedowns and monitoring. Compliance, however, is patchy—especially on encrypted platforms where lawful interception remains technically limited.

Together, these initiatives reflect a fragmented but evolving response—highlighting both the seriousness with which India approaches disinformation and the structural deficits still to be overcome.

g. Way Forward: Strengthening India's Resilience to Disinformation

Countering disinformation requires more than piecemeal responses. It demands a comprehensive strategy that is ethical, institutional, and technologically robust. India's way forward can be visualised through six interlinked pillars.

- **Embedding Digital & Media Literacy in Education**
    - A nationwide "Digital Hygiene" movement is required, akin to the Swachh Bharat campaign.
    - NCERT curricula and training modules for Panchayati Raj leaders and civil servants (e.g., LBSNAA) should integrate lessons on news verification, use of fact-checking sites (AltNews, PIB, BoomLive), and recognising echo chambers or bot-driven amplification.
- **Developing Indian AI Tools for Multilingual Fact-Checking**
    - Given India's linguistic diversity, indigenous AI must detect viral falsehoods across languages, analyse metadata to geo-locate fabricated events, and identify manipulated audio-visuals.
    - Integration with the Election Commission's monitoring, CERT-In alerts, and PIB dashboards would enhance institutional responsiveness.
- **Criminalising Deepfakes with Graded Offences**
    - A dedicated law should define deepfakes, categorise offences by intent and harm, and specify proportional penalties.
    - Provisions must include satire exemptions, harsh sanctions for defamation or fraud, "right to be forgotten" protections, and strict takedown timelines.
- **Institutional Oversight via a Digital Media Commission**
    - An independent, non-partisan body comprising legal experts, technologists, journalists, and civil society members should oversee platform algorithms, political advertising, and content takedowns.
    - Annual transparency reports on takedown volumes, deepfake detection, and grievance resolution would enforce accountability.
- **Enhancing Law Enforcement Preparedness**
    - Cyber cells must be upgraded with AI-based forensic tools, shared dashboards, and SOPs for monitoring.
    - Magistrates, prosecutors, and investigators need structured training in digital evidence handling and media forensics.
- **Strengthening Global Cyber Norms**
    - India must collaborate on AI watermarking standards, UN-led frameworks against information warfare, and cross-border takedown treaties.

- Participation in initiatives such as the EU's *Code of Practice on Disinformation* or the US-led *Countering Digital Authoritarianism Coalition* would bolster India's resilience and shape global norm-setting.

As one observer noted with stark clarity: *"In a democracy, the threat of fake news is greater than the fake bullet. Because it kills judgment, not just people."*

Conclusion

The analysis of disinformation and deepfake ecosystems reveals that the battleground has shifted from the realm of ideas to the architecture of digital platforms. Combating falsehood requires not only literacy and detection tools but also proactive regulatory presence within the very networks that manufacture and spread narratives.

This progression raises a pressing question: how should the state engage with social media platforms whose algorithms can amplify both empowerment and extremism? For India, the answer lies in developing models of social media policing that balance surveillance with rights, accountability with innovation, and state authority with democratic freedoms.

It is to this complex and contested arena of social media regulation and policing that we now turn.

6.3 Social Media Policing in India

a. Introduction

With more than 880 million citizens active on social media, India has become one of the world's largest digital societies. This vast ecosystem generates unprecedented opportunities for communication and participation, but it also poses immense challenges for law enforcement. Traditional policing—designed for physical spaces—is ill-suited to monitor the speed, scale, and complexity of harmful online content.

In response, India has developed hybrid models of social media regulation that integrate technology platforms (Twitter/X, Facebook, YouTube), government agencies (MHA, MeitY), fact-checking organisations, civil society initiatives, and citizen volunteers. These models reflect the recognition that *"law and order in the twenty-first century depends as much on server rooms as on streets."*

b. Major Initiatives in Social Media Policing

- **Twitter Samvad (2015–pilot, now inactive)**
  - *Objective*: Collaboration with Twitter to deliver government and police tweets as SMS alerts during emergencies, riots, or disasters—even in low-internet zones.
  - *Strengths*: Enabled two-way communication, bypassed internet barriers by reaching SMS-only phones, and ensured continuity of messaging during internet shutdowns.
  - *Limitations*: Adoption remained limited; it relied heavily on Twitter's API and SMS gateways, and was eventually phased out.
- **Cyber Volunteer Programme (under I4C, Ministry of Home Affairs)**
  - *Objective*: Crowdsource vigilance by allowing registered citizens to flag unlawful content (e.g., child pornography, terrorist propaganda, hate speech) and promote cyber awareness.

- *Strengths*: Mobilised India's vast online base for real-time reporting; supported cyber hygiene campaigns; acted as a force multiplier for under-resourced cyber cells, especially in smaller towns.
- *Concerns*: Risks of vigilantism, overreporting, and political profiling; fears of misuse against dissent. Lack of transparency on processing flagged content has raised accountability concerns. Human Rights Watch and civil society groups have flagged potential misuse.

- **Fact-Checking Cells**
  - *Government-led*: PIB Fact Check Unit (2019), accredited by the International Fact-Checking Network, verifies misinformation on government policies. States like Maharashtra, Kerala, and Delhi have regional fact-check desks for local-language content.
  - *Legal Controversy*: The IT Rules Amendment (2023) empowered PIB's Fact Check Unit to label content as "false or misleading," mandating takedown by platforms. Critics warn this grants excessive censorship power without judicial or independent oversight.
- **Independent Fact-Checkers**
  - Organisations such as AltNews (communal and political claims), BoomLive (multilingual video fact-checks, partnered with Meta), Factly, and SMHoaxSlayer play critical roles.
  - Their credibility rests on independence, transparent methods, and consistent debunking of politically sensitive disinformation—filling gaps left by limited government outreach.

c. Legal and Regulatory Support

India's social media policing is anchored in a layered legal framework:

- **Section 69A, IT Act**: Empowers the government to block content that threatens sovereignty, security, or public order.
- **Intermediary Guidelines (2021)**: Mandate grievance officers, traceability of harmful content's "first originator," and removal of flagged content within 36 hours—creating accountability but also imposing heavy compliance burdens.
- **IT Rules Amendment (2023)**: Grants government-designated fact-check units authority to order takedowns of "fake or misleading" content related to the government. While aimed at curbing falsehoods, critics argue it risks executive overreach, curbs free speech, and undermines due process.

These provisions illustrate India's evolving regulatory approach—one that blends innovation and state authority but must tread carefully between security imperatives and constitutional freedoms.

d. Challenges in Social Media Policing

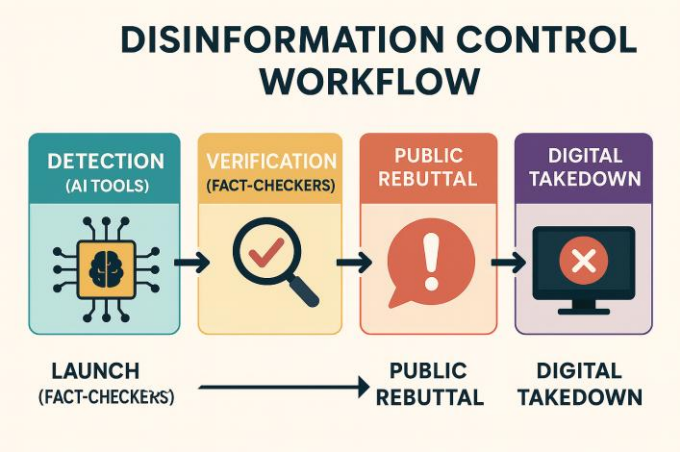
Despite growing institutional efforts, India's approach faces multiple systemic, technological, legal, and ethical constraints.

- **Jurisdictional and Sovereignty Constraints**: Major platforms (Meta, X, YouTube, Telegram) are headquartered abroad, invoking foreign data protection laws (e.g., GDPR). Compliance with Indian takedown requests is often delayed. During the CAA protests and 2020 Delhi riots, inflammatory content persisted online despite government requests for removal.
- **Volume–Velocity–Virality Challenge**: Over 500 million WhatsApp messages are exchanged daily, alongside reels, memes, and tweets. The sheer scale outpaces monitoring capacity; limited multilingual moderation tools mean intervention usually comes *after* unrest begins.
- **Encrypted and Closed Platforms**: End-to-end encryption on WhatsApp, Signal, and Telegram creates opaque spaces where law enforcement has limited visibility. Metadata is rarely shared; origin tracing is difficult without device seizure, weakening preventive policing.

- **Technological Gaps in Law Enforcement**: Many state cyber cells lack advanced tools to detect bot networks, coordinated inauthentic behaviour, or AI-generated content (deepfakes, voice clones). Reliance on manual screenshots, FIRs, and sporadic technical help persists.
- **Ethical and Free Speech Concerns**: Powers under Section 69A and the IT Rules (2023) have raised fears of overreach. Content flagged as "false" can be subjective if adjudicated by politically aligned units, risking suppression of dissent or satire.
- **Polarised and Politicised Ecosystem**: Political IT cells actively disseminate communal or misleading content. If social media policing appears selective, it risks eroding trust and fuelling perceptions of digital authoritarianism.

e. Best Practices and Suggestions

To navigate the challenges of social media policing, India must adopt a rights-respecting, technologically empowered, and multi-stakeholder model of digital governance.



- **Strengthen Cyber Policing Infrastructure**
  - Establish dedicated *Social Media Threat Monitoring Units* in every state.
  - Equip them with AI dashboards capable of detecting trending hate hashtags, viral deepfakes, and coordinated bot activity.
  - Train police personnel in OSINT (open-source intelligence), digital forensics, and techniques for lawful encryption circumvention.
- **Promote Digital Literacy and Civic Awareness**
  - Launch national campaigns such as *"Think Before You Share"*, similar to the Election Commission's voter awareness drives.
  - Integrate media literacy into school curricula to prepare students to critically evaluate online information.
  - Involve religious and community leaders in workshops to build grassroots credibility and reach.
- **Regulate Platforms with Independent Oversight**
  - Establish an independent *Digital Media Commission* comprising legal experts, technologists, journalists, and civil society representatives.
  - Empower the commission to review takedown decisions, oversee algorithmic transparency, and prevent arbitrary censorship.
  - Mandate platforms to publish regular transparency reports detailing flagged and removed content, broken down by language and geography.
- **Legally Define Deepfakes and Penalise Disinformation**
  - Amend the Information Technology Act or enact a new *Digital Harms Law* to clearly define categories such as deepfakes, synthetic pornography, hate speech, and algorithmic amplification of harmful content.
  - Introduce graded penalties—from warnings to fines and imprisonment—with strong appeal mechanisms to prevent misuse.
- **Advance Global Tech Diplomacy for Platform Compliance**
  - Pursue bilateral agreements with the United States and the European Union to expedite access to data and enforce takedown requests.

- Promote international standards on disinformation via forums like the United Nations and the Quad—positioning India as a *norm-setter* rather than a passive rule-follower.

- **Foster Public–Private–Civil Society Collaboration**
  - Integrate NGOs, fact-checking bodies, and civil rights groups into content monitoring protocols to enhance credibility and reduce risks of state overreach.
  - Establish helplines for victims of trolling, deepfake abuse, or online harassment to build public trust in digital policing.

Conclusion

Social media has become both the new public square and the new battlefield. With over 400 million active users in India, platforms can shape discourse, mobilise protests, or destabilise harmony at viral speed. This makes responsive, ethical, and technologically capable digital policing an urgent necessity.

Yet, the dangers of overreach are equally real:

- Security without accountability risks sliding into surveillance.
- Content moderation without safeguards risks degenerating into censorship.

The constitutional balance must therefore remain paramount—protecting freedom of expression under Article 19(1)(a), enforcing reasonable restrictions under Article 19(2), and upholding the sovereign duty of the state to safeguard internal security. The objective is not to silence the *digital street* but to civilise it.

As one commentator noted: *"In the age of algorithmic amplification, the first line of law and order is no longer the beat constable—but the byte custodian."*

India's future lies in creating a digital governance model that is rights-respecting, tech-empowered, and globally coordinated—a framework that secures democracy not by silencing voices but by strengthening the integrity of the information ecosystem itself.

The exploration of India's social media policing highlights both innovation and vulnerability. While fact-checking units, volunteer programmes, and legal provisions provide scaffolding for digital governance, challenges of jurisdiction, encryption, and political polarisation reveal the fragility of this system.

More fundamentally, these issues are not confined to social media platforms alone. Encrypted messengers, gaming forums, and anonymous boards—spaces that lie beyond the reach of conventional oversight—pose an even more formidable challenge.

If social media is the visible frontline of digital disorder, these hidden platforms represent its shadowy hinterland. It is therefore essential to turn next to the structural obstacles of policing such covert digital spaces, which constitute one of the most complex security tasks of the twenty-first century.

6.4 Challenges in Policing Communication Platforms

a. Introduction

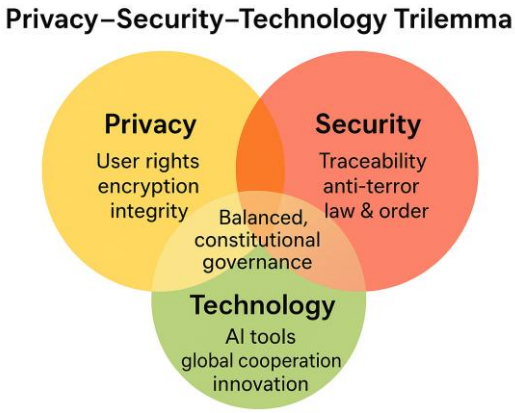
Modern communication platforms have evolved into dual-use infrastructures: empowering free expression and private interaction, while simultaneously providing cover for encrypted terrorist coordination, cross-border propaganda, and misinformation at an unprecedented scale.

The paradox is stark—what strengthens citizen rights can also strengthen criminal capabilities. As one analyst observed: *"A message sent in a second can destabilise a nation for years."*

b. Key Technological Challenges

- **End-to-End Encryption (E2EE)**

- Ensures that only sender and receiver can read messages, excluding even the platform.
- Protects privacy but blinds law enforcement, even with court warrants.
- As per reports, the Pulwama terror attack, coordinated on WhatsApp, illustrates how encryption can shield planning for terrorism, drug trafficking, and organised crime.



- **Jurisdictional Barriers**
  - Major platforms (Meta, X, Telegram) are headquartered abroad.
  - Indian agencies rely on slow Mutual Legal Assistance Treaties (MLATs), often waiting weeks or months for data—by which time accounts may be deleted.
  - Telegram's repeated refusal to cooperate in narcotics and Khalistan-linked cases highlights this weakness.
- **Lack of Traceability**
  - India's 2021 IT Rules mandated tracing the "first originator" of harmful content.
  - Platforms like WhatsApp and Signal resisted, citing risks of undermining encryption and enabling mass surveillance.
  - The issue remains in court, leaving accountability gaps for viral falsehoods.
- **Proliferation of Obfuscation Tools**
  - Parallel apps, cloners, VPNs, TOR browsers, and burner phones allow spoofing of identities and masking of IPs.
  - Widely exploited for darknet operations, narcotics trafficking, and jail-to-street gang communication.
- **Artificial Intelligence–Generated Content and Deepfakes**
  - Cheap and accessible tools enable voice cloning, synthetic videos, and meme automation.
  - Used to incite communal violence, impersonate officials, and radicalise youth.
  - India lacks real-time AI forensic and detection capacity across most states, leaving enforcement reactive.
- **Institutional Gaps**
  - State cyber cells face acute shortages of trained officers in metadata analysis, OSINT, and bot network detection.
  - CERT-IN and other labs remain overstretched, while most states lack advanced forensic tools.
  - Absence of a unified national doctrine on encryption or cyber governance further complicates coordination.

c. Way Forward: Bridging the Technological, Security, and Institutional Gaps

- **Privacy-Respecting Traceability**
  - Platforms could share limited metadata (timestamps, device fingerprints) without exposing message content.

    - Forward-chain analysis may help trace message spread while preserving encryption.
- **Treaty Reforms and Global Cooperation**
    - Modernise MLATs with time-bound digital protocols.
    - Pursue bilateral agreements with the US, EU, and Gulf states for expedited access to critical platform data.
- **Artificial Intelligence–Based Surveillance Tools**
    - Invest in indigenous AI to detect synthetic media, coordinated inauthentic behaviour, and multilingual disinformation.
    - Integrate these tools with CERT-IN, I4C, and the Election Commission.
- **Training for Law Enforcement and Judiciary**
    - Introduce mandatory cyber modules at SVPNPA, state academies, and judicial institutes.
    - Focus areas: OSINT, deepfake detection, blockchain tracing, and attribution methodologies.
- **Public–Private Innovation Partnerships**
    - Establish a *"TechSec Fund"* to support government–industry–start-up collaborations.
    - Prioritise Make-in-India, open-source tools for malware analysis, digital forensics, and disinformation detection.
- **Digital Harms Regulation**
    - Enact a new law to address malicious deepfakes, encryption misuse, and algorithmic amplification.
    - Define thresholds for lawful decryption, mandate takedown audits, and institutionalise judicial review to prevent abuse.

As one policymaker remarked: *"In an encrypted world, national security isn't just about what you can read—it's about what you can trace."*

Conclusion

As India advances towards a trillion-dollar digital economy, internal security increasingly unfolds in encrypted chatrooms, anonymised servers, and synthetic media timelines. Communication platforms have become hybrid spaces: part public square, part propaganda factory, part crime hub. Yet policing models remain rooted in the analogue era—ill-prepared for the velocity and transnational nature of digital threats.

With over 650 million Indians using encrypted apps and deepfake tools available for a few hundred rupees, the window for timely intervention is shrinking. The way forward lies not in blanket bans or unchecked surveillance, but in rule-of-law anchored innovation, predictive policing, and international cooperation.

As one expert warned: *"You do not need a gun to wage war anymore—just code, a camera, and a closed group chat."*

Ultimately, technology alone cannot resolve this dilemma. At its heart, the challenge is one of governance:

- Who has the authority to regulate?
- What powers should they exercise?
- How can individual rights be safeguarded while ensuring state sovereignty?

Having examined the technological and operational challenges, the next step is to turn to the legal architecture—laws, rules, and judicial interpretations—that define India's approach to social media and communication policing.

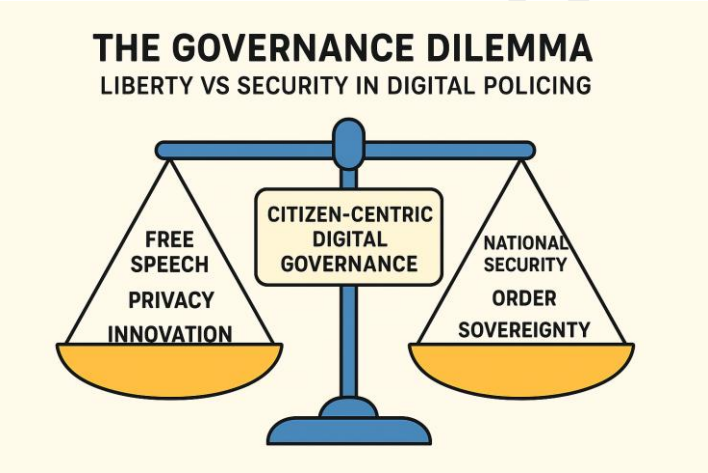
6.5 Legal Framework for Social Media and Communication Policing

a. Introduction

As the digital sphere expands, traditional laws struggle to keep pace. Real-time misinformation, radical content, and anonymous criminal networks evolve faster than the statutes meant to contain them. India's legal framework for social media and communication policing has adapted in response, but gaps persist in enforcement, clarity, and constitutional balance.

The dilemma is aptly captured by the maxim: *"In the digital era, code is law—but the law must still code accountability."*

b. Key Legal Instruments in India



- **Section 69A of the Information Technology Act, 2000**
    - *Provision*: Empowers the central government to block public access to online content if it threatens sovereignty, security, or public order. A designated committee under MeitY reviews requests, and approved takedowns are binding.
    - *Notable Examples*:
        - The 2020 ban on TikTok and 250+ Chinese apps.
        - Blocking of YouTube channels propagating anti-India narratives.
        - Suspension of Twitter handles linked to Khalistani and ISIS propaganda.
    - *Criticism*: Blocking orders are opaque, not disclosed publicly, and lack appeal mechanisms. Civil liberties groups warn of executive overreach with censorship powers concentrated in government hands.
- **Intermediary Guidelines and Digital Media Ethics Code (IT Rules 2021, amended 2023)**
    - Extend to all major intermediaries (Facebook, WhatsApp, Instagram, YouTube, Telegram, X).
    - *Key Provisions*:
        - Appointment of grievance officers in India for coordination.
        - Traceability of harmful content's "first originator."
        - Removal of unlawful content within 36 hours of notice.
        - Self-regulation norms for digital media, requiring OTT and digital news providers to classify content and establish grievance redress bodies.
    - *Assessment*: Together with Section 69A, the IT Rules form the twin pillars of India's legal regime for communication policing, providing mechanisms for blocking, takedown, and compliance enforcement.

c. Criticisms and Constitutional Concerns

Despite their utility, India's legal instruments have sparked debate:

- **Vagueness of Terminology**: Terms like "fake," "offensive," or "misleading" remain undefined, risking arbitrary application.
- **Free Speech vs National Interest**: Critics argue the balance tilts too heavily towards state control, constraining democratic debate.

- **Lack of Judicial Review**: Takedown/blocking orders are largely executive in nature, with no automatic provision for independent oversight or appeal.
- **Impact on Innovation**: Compliance burdens weigh disproportionately on smaller Indian start-ups compared to global tech giants.
- **Judicial Challenges**: The Editors Guild of India and digital rights organisations have petitioned the Supreme Court against the 2023 IT Rules, citing risks to press freedom and unchecked executive power.

d. Suggested Reforms and the Way Forward

India must shift from reactive censorship to principled governance, reforming its legal regime along several axes:

- **Clear Legislative Definitions**
    - Statutes should explicitly define *fake news, disinformation, deepfakes, and hate speech* to reduce arbitrariness.
- **Independent Digital Tribunal**
    - Establish a quasi-judicial body for appeals on takedown decisions, ensuring both citizens and platforms have access to redress.
- **Privacy-Respecting Traceability**
    - Adopt technical protocols like hash-matching and metadata flow mapping to trace harmful content without dismantling encryption.
- **Transparency Mandates**
    - Require platforms to publish regular transparency reports on takedown requests, originator-tracing demands, and user notices.
- **Capacity Building in Law Enforcement**
    - Judges, prosecutors, and police must be trained in cyber law, digital evidence interpretation, blockchain forensics, and disinformation attribution.
- **Global Harmonisation**
    - Align with international best practices such as the EU's *GDPR* and *Digital Services Act* or the UK's *Online Safety Bill*, while tailoring them to Indian conditions.

Conclusion

India's legal framework for social media and communication policing stands at a crossroads. Instruments like Section 69A and the IT Rules have equipped the state with powerful tools to counter digital threats, but they have also intensified concerns over executive overreach, lack of judicial oversight, and opaque enforcement.

According to *Access Now (2023)*, India recorded the highest number of internet takedown requests worldwide—an indicator of both the seriousness of threats and the opacity of state actions.

The challenge is not to create *more law* but to create *better law*: transparent in design, accountable in enforcement, and adaptive in application. In an age where platforms influence politics as much as parliaments, legal frameworks must function like code—precise, auditable, and open to scrutiny.

India's next-generation architecture must therefore move beyond control-centric statutes to citizen-centric governance, securing both state sovereignty and democratic vitality.

The study of communication platforms reveals how the digital sphere has become both the battleground and the bloodstream of modern security challenges. Platforms amplify propaganda, enable coordination, and test the state's ability to regulate without eroding liberty. Yet information warfare is only one side of the coin.

The same networks that radicalise minds and mobilise crowds also channel money, launder illicit wealth, and finance violence. Terrorism, organised crime, and extremist movements cannot survive on

ideology alone—they depend on financial lifelines through hawala networks, shell companies, and increasingly, cryptocurrencies.

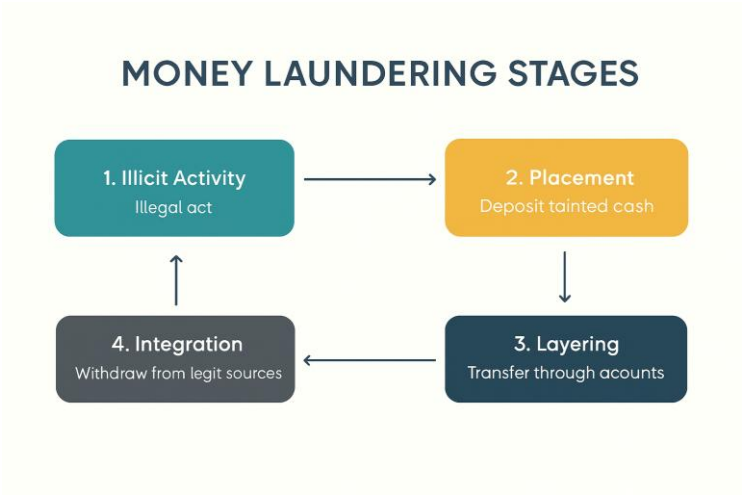
Having examined the informational dimensions of internal security, we now turn to its economic undercurrents: money laundering and terror financing, which sustain and globalise insecurity.

Chapter 7. Money Laundering & Terror Financing

7.1 Money Laundering – Definition & Three-Stage Process

a. Introduction

In any well-functioning democracy, the financial system should serve as a transparent channel for economic growth, public welfare, and regulated commerce. When illicit funds infiltrate these structures, however, they transform into instruments of distortion and danger.



Money laundering refers to the process by which proceeds of crime are disguised to appear legitimate, thereby integrating *"dirty money"* into the formal economy. This enables criminals, terrorists, and corrupt officials to clean their illegal wealth, complicating detection, tracing, and prosecution by enforcement agencies.

Laundering masks the criminal origin of funds through a web of bank transactions, shell companies, property investments, and increasingly, digital assets. Its consequences extend far beyond economics:

- It empowers criminals to enjoy illicit gains.
- It embeds their influence into politics, business, and media.
- It fuels what experts call the criminal–political–financial nexus.

Thus, money laundering is not a mere economic irregularity but a direct threat to national security, economic stability, and democratic governance. As one analyst observed: *"If crime is the engine of the underworld, money laundering is its fuel system."*

From terror financing in Kashmir and fake NGOs in Delhi to benami real estate in Mumbai, laundering constitutes the invisible artery through which illicit power circulates in modern India.

The problem is compounded by four factors:

- The ease of cross-border flows under globalisation.
- The rise of crypto-based laundering and privacy-enhancing wallets.
- Weak enforcement capacity, especially in overburdened financial intelligence units.
- Political protection in cases involving politically exposed persons.

b. Global Perspective

Money laundering is a transnational phenomenon. The UN Office on Drugs and Crime (UNODC) estimates that between 2 and 5 percent of global GDP—equivalent to USD 800 billion to 2 trillion—is laundered each year.

Mechanisms include:

- Shell companies and offshore banking accounts.
- Cryptocurrency mixers and anonymisers.
- Informal value transfer systems such as hawala.

Illicit finance is thus among the most pervasive and resilient features of globalisation.

c. Indian Context

India faces acute vulnerabilities to laundering flows from both domestic and transnational sources:

- **Domestic crimes**: Corruption, tax evasion, electoral funding via fake NGOs, and illegal land transactions.
- **Cross-border syndicates**: Operations of the Dawood Ibrahim network and ISI-backed proxies.
- **Terror modules**: Particularly in Kashmir, Punjab, the Northeast, and Left-Wing Extremist zones, reliant on hawala and cryptocurrencies.
- **Politically exposed persons (PEPs)**: Divert public funds through layered transactions to escape scrutiny.

In India, laundering is therefore not merely an economic crime, but a governance and internal security crisis.

d. The Classic Three-Stage Process of Money Laundering

Stage	What Happens	Illustration / Threats
Placement	Introduction of illicit funds into the financial system via banks, casinos, shell firms, or property.	Breaking large deposits into smaller sums; buying gold/real estate; inflating invoices; false donations.
Layering	Complex transactions obscure the audit trail and sever money from its source.	Transfers through offshore accounts, hawala chains, cryptocurrency mixers, or tax havens (e.g., Mauritius, Dubai).
Integration	Funds re-enter the legitimate economy appearing "clean."	Investments in real estate/start-ups, luxury purchases, political donations, film financing, or NGO grants.

This placement → layering → integration cycle illustrates why laundered funds become so difficult to trace once absorbed into the system.

e. Why This Process is Dangerous for India

- **Terror Financing Enabler**: Laundered funds sustain sleeper cells, purchase arms, and fuel separatist violence.
- **Undermines Internal Security**: ISI-backed networks use counterfeit currency, smuggled gold, and hawala chains to finance insurgencies and radicalisation.
- **Erodes Rule of Law**: Political corruption becomes untraceable once funds are layered offshore.
- **Politicisation of Illicit Wealth**: Electoral bonds, NGOs, and benami media ownership channel black money, undermining electoral integrity and press freedom.
- **Real Estate Inflation**: Black money inflates property prices, distorts urban growth, and entrenches corruption in planning.
- **Criminal–Political Nexus**: Criminals fund political campaigns in return for protection; politicians rely on laundered funds for elections.
- **Revenue Loss**: Tax evasion diverts income into shadow channels, depriving the state of resources.
- **Weakening Public Trust**: Cases such as the 1991 hawala scandal, the *Panama Papers*, and the NSE co-location scam reinforce perceptions of impunity for the powerful.

As one analyst warned: *"Unchecked money laundering transforms the economy into a vehicle for extremism, impunity, and elite capture."*

Conclusion

Money laundering is not merely a financial irregularity—it is the oxygen supply for terrorism, organised crime, and institutional decay. In an era of rapid digitisation and globalisation, India's vulnerabilities have multiplied: hawala corridors, crypto mixers, and shell networks hollow out governance, distort elections, and finance anti-state actors.

The UNODC's estimate—that 2–5% of global GDP is laundered—underscores the systemic scale of the threat. For India, piecemeal crackdowns are insufficient. What is needed is:

- Tighter political financing laws.
- Empowered financial intelligence units and the Enforcement Directorate with global reach.
- A financial intelligence architecture as agile and borderless as the illicit funds it seeks to trace.

As one expert observed: *"The most dangerous currency in a democracy is not money, but unaccounted money."* Unless curbed, laundering will corrode the foundations of internal security, rule of law, and democratic legitimacy.

The three-stage laundering process—placement, layering, and integration—demonstrates how illicit wealth is transformed from *"dirty"* to *"clean."* Yet these stages are not abstract; they operate through concrete pathways that exploit financial systems, trade routes, and informal channels.

From hawala corridors and shell companies to real estate and cryptocurrencies, these conduits are the arteries through which black money flows within and across borders. To grasp the full scope of the threat, it is essential to map these channels and examine how they sustain criminal enterprises, terrorism, and political corruption.

7.2 Channels of Money Laundering

a. Introduction

Money laundering is not a single act but a multi-layered, adaptive process that thrives on the ingenuity of its practitioners. The channels through which it operates have grown increasingly sophisticated, transnational, and technology-driven.

Gone are the days when laundering relied only on cash couriers or shell firms. Today, launderers exploit legal grey zones, informal transfer systems, and digital loopholes to obscure the origins of illicit wealth. From fake invoices in trade to blockchain-based transactions, these channels provide speed, anonymity, and resilience, often outpacing conventional financial surveillance.

Their greatest strength lies in interoperability: illicit funds can originate in India, move through hawala brokers in Dubai, be layered via shell firms in Mauritius, disguised through trade misinvoicing, and integrated abroad via cryptocurrencies—all within hours.

As one analyst cautioned: *"In the digital era, money laundering is not a pipeline—it is a maze with multiple exits, all leading to legitimacy."*

Understanding these channels is vital for financial integrity, national security, democratic accountability, and international credibility. Four channels dominate both the Indian and global laundering landscape.

i. Shell Companies and Benami Entities

- **Nature**: Shell companies are firms that exist on paper without substantive operations. They are designed to move, layer, or park illicit money. Criminals and politically exposed persons often set them up using proxies or relatives.
- **Mechanisms**: Fake invoices, sham loans, or bogus business deals conceal the true origin of funds.
- **Dangers**: Widely used in political funding, real estate deals, and fraudulent investments. Their opacity makes it nearly impossible to trace ultimate beneficiaries, often enabling corporate lobbying or regulatory capture.
- **Case Illustration**: Fugitive businessmen such as *Nirav Modi* and *Vijay Mallya* relied on overseas shell firms to layer funds and evade Indian jurisdiction.

ii. Hawala Networks

- **Nature**: Hawala is an informal, trust-based value transfer system that bypasses formal banking channels. Common in South Asia and the Middle East, it enables near-instant transfers without physical money movement.
- **Mechanism**: A person in Delhi deposits funds with broker X; a counterpart in Dubai or London pays the recipient. Balances are maintained through ledgers, coded diaries, or encrypted chats.
- **Threats**: Hawala is unregulated, untraceable, and extremely fast, making it a preferred channel for terror financing, drug trafficking, corruption, and organised crime.
- **Complication**: It often overlaps with genuine diaspora remittances and is shielded by political patronage.
- **Investigator's Remark**: *"Hawala is the bloodstream of underground economies."*

iii. Trade-Based Money Laundering (TBML)

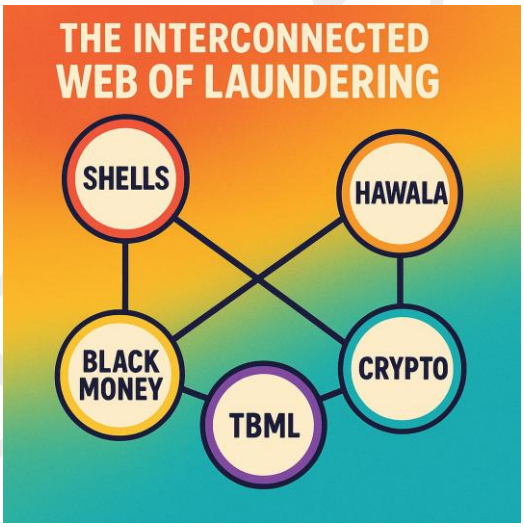
- **Nature**: TBML disguises illicit funds through manipulation of legitimate trade transactions.
- **Techniques**:
    - Over-invoicing exports to justify inflows of foreign exchange.
    - Under-invoicing imports to evade taxes and channel black money.
    - Misclassifying commodities or generating phantom shipments.
- **Vulnerable Sectors**: Diamonds, gold, electronics, textiles, pharmaceuticals, and chemicals—industries with high value and complex supply chains.
- **Impacts**: TBML distorts trade statistics, enables tax evasion, undermines genuine businesses, and erodes India's credibility in global markets.
- **Illustration**: Profits from Afghanistan's heroin trade were laundered via fabricated textile exports, masking narcotics proceeds as trade revenue.

iv. Cryptocurrency and Blockchain-Based Laundering

- **Nature**: Cryptocurrencies like Bitcoin, Ethereum, Monero, and Tether are replacing hawala as preferred mediums for anonymous transfers. They facilitate cross-border laundering, terror financing, and dark web transactions.
- **Method**: Illicit cash is converted into crypto via peer-to-peer traders or unregulated exchanges, dispersed across wallets in micro-payments, and cashed out abroad.
- **Challenges**:
    - Pseudonymous wallets mask identities.
    - Privacy coins (e.g., Monero) obscure trails.
    - Crypto mixers fragment transactions beyond traceability.
    - Many exchanges operate offshore, outside Indian jurisdiction.

- **Indian Legal Status**:
    - Cryptocurrencies remain legal but unregulated.
    - RBI's 2018 ban was overturned by the Supreme Court (2020).
    - The Financial Intelligence Unit mandates KYC compliance for exchanges.
    - Union Budget 2022 imposed a 30% tax on crypto income.
- **Emerging Trends**:
    - Blockchain bridges allow swaps across networks.
    - Decentralised finance (DeFi) platforms enable anonymous lending.
    - Terror groups solicit crypto donations via QR codes on Telegram.
    - NFTs and gaming tokens are being misused to mask illicit assets.
- **Expert's Warning**: *"Cryptocurrency has created a parallel banking universe—decentralised, borderless, and dangerously opaque."*

Conclusion



Money laundering rarely relies on a single channel. A single rupee of illicit wealth may pass through hawala corridors, shell firms, trade misinvoicing, and cryptocurrency wallets before returning "clean" to India.

This ecosystem is dangerous not only because of its speed and anonymity but also because of its global reach, which keeps launderers perpetually ahead of enforcement. Analysts rightly warn: *"The ingenuity of money launderers is often one step ahead of enforcement—unless laws, technology, and global cooperation catch up."*

For India, countering these channels requires:

- Real-time data sharing across agencies.
- International treaty reforms for faster cooperation.
- Proactive financial intelligence systems that can match the borderless pace of illicit flows.

The study of laundering channels—shell firms, hawala, TBML, and crypto—shows how illicit funds weave through multiple pathways before integration into the formal economy. But understanding the methods is only half the challenge. For policymakers, the pressing question is scale:

How much dirty money actually flows through India's financial system, and how far do official statistics reflect the ground reality?

To answer this, we must now turn from mechanisms to measurement, assessing the true extent of money laundering in India through statistics, reports, and enforcement experiences.

7.3 Extent of Money Laundering in India: Official Estimates, Reports and Ground Realities

a. Introduction

Money laundering in India is not merely an economic offence; it is a strategic threat that corrodes governance, fuels terrorism, and erodes public trust in institutions. Laundered funds form the financial backbone of corruption, drug trafficking, insurgency, and opaque electoral practices.

Precise measurement is elusive, given the covert and transnational nature of illicit flows. However, data from the Financial Intelligence Unit (FIU-IND), the Enforcement Directorate (ED), the Reserve Bank of India (RBI), and other agencies reveal both the magnitude and the systemic depth of the problem.

With black money coursing through shell companies, hawala networks, trade misinvoicing, and cryptocurrencies, the extent of laundering is measured not only in rupees lost but also in the erosion of transparency, accountability, and democratic integrity.

b. Official Estimates and Statistics

- **FIU-IND**: Received over 500,000 Suspicious Transaction Reports (STRs) in 2022–23, the highest proportion originating from banks, followed by NBFCs, mutual funds, and crypto exchanges. Many flagged narcotics-linked flows, shell firms, suspect NGOs, and terror financing.
- **Enforcement Directorate (ED)**: As of 2023, registered 5,400+ PMLA cases since inception. Assets worth ₹1.15 lakh crore provisionally attached, but fewer than 35 convictions secured—reflecting a conviction rate under 1%. High-profile cases include the *Rose Valley ponzi scam, Popular Front of India probe, coal scam, illegal sand mining, and Delhi liquor policy case*.
- **Reserve Bank of India (RBI)**: Avoids direct estimates but studies suggest 20–30% of GDP operates in the black economy, part of which is laundered. RBI has flagged misuse of cooperative banks, hawala networks, and shell entities.
- **Income Tax Department (CBDT)**: Between 2014–23, detected ₹1.96 lakh crore in unaccounted income. Over 10,000 benami transactions remain under investigation.
- **NITI Aayog**: Policy papers highlight real estate, gold trade, education trusts, and electoral funding as high-risk sectors. Recommendations include linking land registries with FIUs and expanding analytics-driven oversight.

c. International Reports and Indices

- **Financial Action Task Force (FATF)**: The 2010 mutual evaluation flagged gaps in India's NGO oversight, cross-border cash controls, and crypto regulation. India exited FATF follow-up in 2013 after corrective action, though vulnerabilities persist.
- **Global Financial Integrity (GFI)**: Estimated that India lost $88 billion annually (2008–2017) through illicit outflows, primarily via trade misinvoicing and capital flight.
- **US State Department (2022)**: Classified India as a *"jurisdiction of concern"*, citing widespread hawala use, real estate laundering, and shell company abuse.
- **Transparency International (2023)**: Ranked India 93rd of 180 countries in the Corruption Perceptions Index, reflecting the nexus of laundering, political corruption, and weak enforcement.

d. Sector-Wise Red Flags

Findings from the ED, CBI, and RBI highlight recurring vulnerabilities:

- **Real Estate**: Over/under-valuation, benami land deals, and shell buyers absorb illicit wealth.
- **Gold & Jewellery**: Cash-heavy transactions, anonymous resale, and smuggling make it a preferred value store.

- **Cryptocurrency**: Pseudonymous wallets, privacy coins, and P2P exchanges facilitate anonymity; early weak KYC norms worsened risks.
- **Charities & NGOs**: Fake donations and misused foreign contributions cloak laundering, occasionally linked to extremist or political networks.
- **Political Funding**: Electoral bonds and opaque donations integrate black money into campaigns.
- **Trade-Based Laundering**: Over-invoicing, under-invoicing, and phantom shipments distort trade and legitimise illicit flows.

As one analyst remarked: *"India does not just lose money through laundering—it loses transparency, trust, and control over its democratic and financial institutions."*

Conclusion

Money laundering in India is deeply entrenched, spanning both informal economies and formal institutions. Despite high-profile seizures and investigations, the PMLA conviction rate below 1% reveals not just enforcement bottlenecks but also judicial and procedural fragility.

The scale of the problem is reflected in FIU's receipt of half a million STRs in a single year. Yet seizures and arrests alone cannot restore public confidence. As one observer noted: *"India does not just lose money through laundering—it loses trust, control, and constitutional integrity."*

To move beyond shadow-chasing, India must:

- Strengthen inter-agency coordination.
- Tighten regulation of political and NGO financing.
- Forge global partnerships for intelligence sharing.
- Build institutional capacity for forensic, legal, and judicial follow-through.

The extent of laundering—revealed in official statistics and global reports—underscores that the problem is less about recognition and more about response. Confronting it requires a robust architecture of financial intelligence, cross-border cooperation, regulatory enforcement, and judicial efficiency.

Having mapped the scale and scope of laundering, it is now essential to examine the institutional mechanisms—national and international—that India relies upon to combat money laundering and terror financing.

7.4 Institutional Mechanisms to Tackle Money Laundering and Terror Financing

a. Introduction

Illicit financial flows are inherently globalised, fluid, and networked. They thrive on weak borders, legal loopholes, and fragmented enforcement. To counter this, India relies on a layered ecosystem of national agencies and international partnerships tasked with detection, investigation, prosecution, intelligence-sharing, and compliance monitoring.

The effectiveness of this system depends not only on institutional mandates but also on their ability to coordinate, innovate, and adapt to adversaries who are perpetually one step ahead.

i. Enforcement Directorate (ED)

- **Role**: India's principal agency for investigating and prosecuting money laundering and foreign exchange violations. Operates mainly under the *Prevention of Money Laundering Act, 2002 (PMLA)* and the *Foreign Exchange Management Act, 1999 (FEMA)*.

- **Powers**: Can attach, seize, and confiscate proceeds of crime, arrest suspects, and prosecute offenders. Investigations begin with an *Enforcement Case Information Report (ECIR)*, akin to a criminal FIR.
- **High-Profile Cases**: The 2G spectrum scam, Nirav Modi and Vijay Mallya fugitive cases, the Popular Front of India probe, and illegal mining scandals.
- **Challenges**:
    - Conviction rate under 1%, reflecting legal complexity and procedural gaps.
    - Accusations of political misuse and selective targeting.
    - Jurisdictional overlaps with the CBI and Income Tax Department.

ii. Financial Intelligence Unit – India (FIU-IND)

- **Role**: Nodal agency for financial intelligence; central to India's anti–money laundering architecture.
- **Inputs**: Receives Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs), and intelligence feeds from banks, NBFCs, mutual funds, insurance firms, and now cryptocurrency exchanges.
- **Outputs**: Disseminates analysed intelligence to enforcement agencies like ED, NIA, and CBI.
- **Recent Action**: In 2023, issued show-cause notices to global crypto exchanges such as *Binance* and *KuCoin* for non-compliance with Indian AML norms.
- **Significance**: Serves as India's financial radar and connects with international platforms such as the Egmont Group.

iii. Financial Action Task Force (FATF)

- **Nature**: Established in 1989, headquartered in Paris, FATF is the leading inter-governmental body combating money laundering, terror financing, and proliferation financing.
- **India's Status**: Became a full member in 2010—boosting legitimacy and diplomatic leverage.
- **Mandates**: Issues 40 global recommendations; conducts mutual evaluations and compliance reviews.
- **Influence**: FATF's "grey list" and "black list" wield powerful diplomatic pressure, as seen in Pakistan's grey-listing—an outcome India leveraged.
- **Benefits for India**: Membership has strengthened KYC norms, tightened oversight on cryptocurrencies, and aligned domestic laws with international benchmarks.

iv. Egmont Group

- **Nature**: A network of 170+ financial intelligence units enabling secure international cooperation. India's FIU has been a member since 2007.
- **Functions**: Facilitates cross-border exchange of STRs, develops typologies of laundering/terror finance, and builds capacity for digital tracking.
- **Significance**: Bypasses slow diplomatic channels, allowing India to access intelligence on fugitives, foreign assets, and terror financing trails. Serves as a bridge between domestic surveillance and global enforcement.

Conclusion

India's fight against money laundering and terror financing is anchored in this ecosystem of institutions and partnerships:

- The ED provides investigative teeth.
- The FIU-IND functions as the financial radar.
- The FATF shapes global compliance norms.
- The Egmont Group enables real-time intelligence exchange.

Together, they form a scaffold for India's response to financial crime. Yet vulnerabilities persist: low conviction rates, political contestation, and technological gaps. As one analyst noted: *"In the age of globalised crime, data is currency—and cooperation is the only defence."*

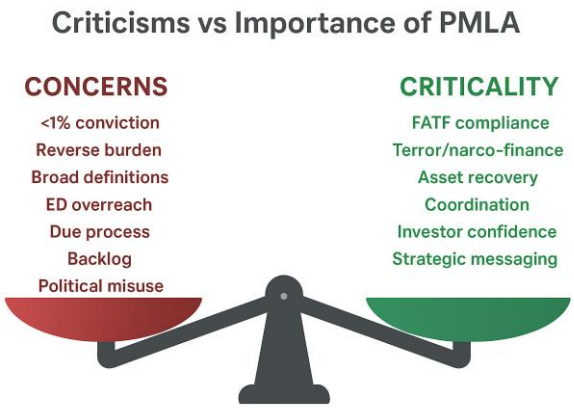
Moving from reactive prosecution to proactive deterrence will require institutional synergy, legislative reform, and tech-enabled monitoring that can keep pace with launderers' ingenuity.

The institutional architecture—ED, FIU-IND, FATF, and the Egmont Group—shows how India blends domestic capacity with global partnerships. But institutions derive their power from law. At the heart of India's AML/CTF regime lies the Prevention of Money Laundering Act, 2002 (PMLA)—a statute that has evolved through successive amendments to address threats from hawala to cryptocurrencies.

Having mapped the institutions, we now turn to the PMLA, the law that empowers them with both authority and controversy.

7.5 Prevention of Money Laundering Act (PMLA), 2002 and Amendments

a. Introduction



In an era of globalised finance and transnational crime, money laundering has emerged as a silent but powerful enabler of terrorism, organised crime, and political corruption. To counter this, India enacted the Prevention of Money Laundering Act (PMLA), 2002, establishing the country's principal legal framework to trace, attach, and confiscate proceeds of crime.

The PMLA is not merely an economic safeguard; it is both a national security instrument and a compliance mechanism for India's obligations under global regimes such as the Financial Action Task Force (FATF). It arms enforcement agencies with formidable powers—arrest without prior judicial sanction, attachment of property, and even reversal of the burden of proof.

Yet, these sweeping powers have triggered debate. Critics highlight constitutional concerns, alleged selective targeting, and persistently low conviction rates. As one commentator remarked: *"If black money is the disease, the PMLA is India's legal immune system—powerful, but not without side effects."*

b. Objectives of the PMLA

The Act was designed with four core objectives:

- **Prevention and Control** of money laundering as a national security and economic integrity imperative.
- **Confiscation of Property** derived from or involved in laundering, denying criminals the fruits of their crime.
- **Punishment of Offenders** with imprisonment from three to seven years, extendable to ten in narcotics-related cases.
- **Institutionalisation of Compliance**, through mandatory reporting of suspicious transactions, freezing of assets, and international cooperation in financial investigations.

c. Major Provisions of the PMLA

- **Scheduled Offences**: PMLA is invoked only when the predicate offence is listed in its schedule, covering corruption, narcotics, arms trafficking, terrorism, and even wildlife smuggling.
- **Attachment of Property**: ED may provisionally attach assets (movable or immovable) suspected of being linked to laundering, subject to confirmation by an adjudicating authority.
- **Search, Seizure, and Arrest**: ED can raid premises, seize documents, and arrest suspects without prior court permission.
- **Burden of Proof**: Reverses the presumption of innocence—the accused must prove assets are legitimate, striking at the anonymity of illicit wealth.
- **Reporting Entities**: Banks, NBFCs, mutual funds, insurance firms, and crypto exchanges are mandated to file Suspicious Transaction Reports (STRs) and Cash Transaction Reports (CTRs) with FIU-IND.
- **Special Courts**: Established for PMLA trials to ensure expertise and speed, though delays remain significant in practice.

d. Key Amendments Over Time

- **2009**: Expanded scope to include cross-border crimes; widened list of scheduled offences.
- **2012**: Introduced the term *"proceeds of crime"*, covering possession and concealment; enabled confiscation of equivalent assets even abroad.
- **2019**: Elevated money laundering into a stand-alone offence, not dependent solely on scheduled crimes; allowed limited retrospective application.
- **2023 (via Finance Act)**:
    - Strengthened ED's power to summon and record statements.
    - Expanded laundering definition to include *attempts, concealment, and possession.*
    - Clarified simultaneous application of NDPS Act, PMLA, and UAPA.

The PMLA has become India's most powerful legal weapon against illicit financial flows. Its provisions on surveillance, seizure, and prosecution make it indispensable in tackling the complex nexus of corruption, organised crime, and terror financing.

e. Criticisms and Concerns Regarding the PMLA

While the Act serves a crucial national and international function, it has attracted persistent scrutiny for its design, implementation, and potential overreach:

- **Low Conviction Rate**: As of 2023, out of 5,400+ registered cases, fewer than 25 secured conviction—reflecting a conviction rate under 1%. Critics argue the Act functions more as an instrument of deterrence and intimidation than effective prosecution.

- **Reversal of Burden of Proof**: Section 24 presumes guilt unless the accused proves legitimacy of assets. This departs from criminal jurisprudence norms, placing disproportionate responsibility on individuals even before trial.
- **Broad Definitions**: The phrase *"proceeds of crime"* extends even to assets merely *"used in connection with"* laundering. This enables action against individuals in possession of such assets, regardless of proof of direct involvement.
- **Unrestrained ED Powers**: The Enforcement Directorate can conduct searches, seizures, and arrests without prior judicial sanction. Grounds for arrest need not be disclosed immediately, raising risks of arbitrary detention.
- **Due Process Concerns**: Provisions often clash with Article 14 (equality before law) and Article 21 (personal liberty). Bail is especially onerous due to "twin conditions," leading to prolonged pre-trial detentions.
- **Judicial Backlog**: Special PMLA courts are heavily overburdened. In several high-profile cases, property attachments have persisted for years without conviction.
- **Political Misuse Allegations**: A disproportionately high number of PMLA cases involve opposition leaders, journalists, and activists. Investigations often intensify during election seasons, fuelling fears of selective targeting.

f. Why PMLA Remains Critical

Despite controversies, the PMLA remains indispensable in India's anti-laundering arsenal, for six reasons:

- **Fulfilling Global Commitments**: As an FATF member, India must uphold stringent AML/CTF standards. PMLA ensures compliance with FATF's 40 recommendations, especially on terror and proliferation finance.
- **Combating Complex Threats**: Invoked in cases involving narco-terrorism, hawala corridors, crypto laundering, and cross-border terror financing, PMLA provides a legal framework to disrupt flows originating in Pakistan, the Gulf, and Southeast Asia.
- **Linking Predicate Offences**: By connecting predicate crimes (e.g., narcotics, corruption, arms smuggling) with laundering, the Act allows investigators to build a composite financial trail across jurisdictions.
- **Institutional Coordination**: PMLA creates a common platform for ED, FIU-IND, CBI, NIA, and global networks like Interpol and the Egmont Group, enabling seizures, extradition requests, and joint probes.
- **Asset Recovery and Deterrence**: Enabled attachment and confiscation of assets worth thousands of crores. In high-profile cases (Nirav Modi, Vijay Mallya, Rose Valley), assets exceeding ₹18,000 crore were attached—striking at financial incentives.
- **Strategic Messaging**: Beyond enforcement, PMLA signals India's resolve against corruption and terror finance, bolstering investor confidence and strengthening leverage in tax treaties and extradition diplomacy.

Conclusion

The PMLA is among India's most potent legal instruments against financial crime linked to terrorism, narcotics, and grand corruption. Yet its sweeping powers and conviction rate under 1% raise pressing questions of constitutional propriety and fairness.

As of 2023, the ED had attached assets worth over ₹1.15 lakh crore, but convictions numbered fewer than 35. This stark disparity reflects both the Act's deterrent strength and its procedural weaknesses.

As one legal scholar observed: *"The strength of a democracy is tested not only in punishing corruption, but in how fairly it does so."*

For legitimacy, the PMLA must evolve to:

- Balance enforcement with liberty.
- Improve institutional transparency.
- Guarantee equal application across the political spectrum.

Only then can it serve not merely as a shield against illicit wealth, but also as a standard of fair justice in India's democratic arsenal.

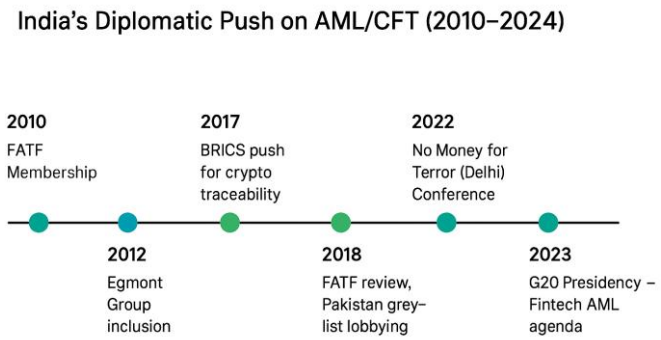
The PMLA has given India a strong domestic weapon to counter illicit flows. Yet laundering and terror financing are rarely confined within borders. Hawala corridors span South Asia and the Gulf; shell firms are incorporated offshore; cryptocurrencies move seamlessly across jurisdictions. No matter how robust, domestic legislation is only one piece of the puzzle.

India's credibility and effectiveness also depend on its standing in global regimes—FATF, Egmont Group, and emerging frameworks on crypto and digital assets. Having examined the domestic law, it is now necessary to assess India's global position in the fight against money laundering and terror financing, and how it balances sovereignty with international obligations.

7.6 India's Global Position on Money Laundering and Terror Financing

a. Introduction

Money laundering and terror financing today transcend geography and traditional banking. They operate through multinational shell networks, encrypted cryptocurrencies, and manipulations of cross-border trade.



For India—an emerging economic power and a full member of the Financial Action Task Force (FATF)—this dual reality presents both a strategic challenge and a diplomatic opportunity.

India's anti-laundering strategy has evolved from a domestic focus under statutes such as the *Prevention of Money Laundering Act (PMLA)* and the *Unlawful Activities Prevention Act (UAPA)* to active engagement in global institutions, bilateral treaties, and fintech diplomacy.

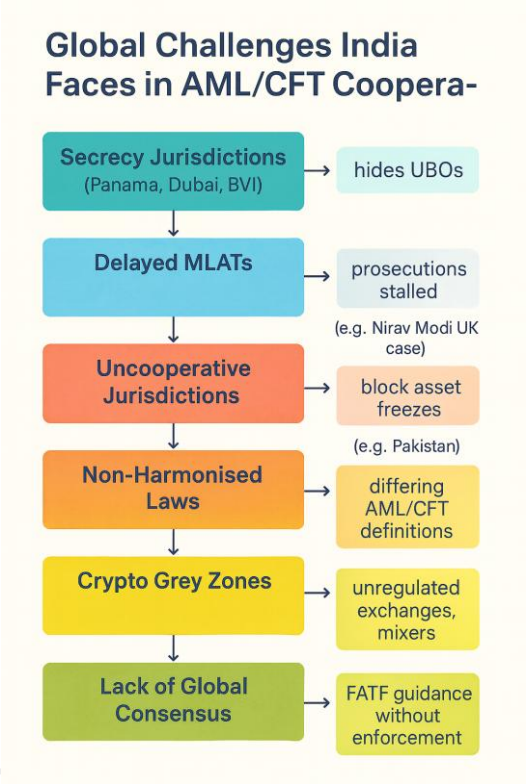
Through its participation in the FATF, Egmont Group, G20, and the "No Money for Terror" (NMFT) process, India has positioned itself not only as a compliant state but also as a norm-shaper. It consistently raises concerns about:

- State-sponsored terror financing.
- Misuse of cryptocurrencies and digital assets.
- The global imperative of financial transparency.

Yet challenges remain. Secrecy jurisdictions, legal asymmetries, and geopolitical inertia continue to shield illicit flows. India's task is therefore to lead with a blend of legal innovation, cooperative resolve, and strategic diplomacy.

b. India's Role in Global AML/CFT Bodies

- **Financial Action Task Force (FATF)**: India became a full member in 2010. Membership strengthened domestic AML/CTF laws and enhanced diplomatic leverage. India has also used FATF's *grey-listing mechanism* to pressure Pakistan on terror financing.
- **Egmont Group**: FIU–India has been a member since 2007, enabling real-time intelligence sharing with over 170 countries. This bypasses slow bilateral channels, allowing access to STRs and laundering typologies.
- **Asia/Pacific Group on Money Laundering (APG)**: India contributes to compliance reviews, capacity-building, and developing regional typologies.
- **Interpol, UNODC, and the G20**: India participates in joint task forces, UN conventions, and financial stability processes. These forums connect anti-laundering measures to broader goals of security, development, and governance of global finance.



c. Key Diplomatic Platforms and Conferences

- **No Money for Terror (NMFT) Conference**: India hosted the 2022 summit in New Delhi, with delegates from 70+ nations. India called for:
  - Cutting terror financing at the source.
  - Holding states accountable for sponsorship.
  - Stronger oversight on cryptocurrencies, NGOs, and charities.
- **UN Conventions**: India has ratified the *United Nations Convention against Corruption (UNCAC)* and the *United Nations Convention against Transnational Organized Crime (UNTOC)*. It advocates robust frameworks for asset recovery and financial crime prosecution.
- **BRICS, SCO, and Quad Dialogues**: In multilateral forums, India pushes for FATF compliance, cryptocurrency traceability, and harmonised norms for cross-border prosecution. These groupings allow India to balance ties between Western democracies and non-Western partners.
- **Extradition Treaties and MLATs**: India maintains over 45 active treaties, enabling cooperation in investigating and prosecuting financial crimes. While often slow, these remain essential for bringing fugitives and assets back under Indian jurisdiction.

d. Challenges in India's Global Engagement on AML/CFT Issues

Despite extensive reforms at home, India's global engagement on anti–money laundering and counter–terror financing continues to face formidable obstacles. These arise from weak international law, secrecy jurisdictions, uncooperative states, and fast-evolving technology.

- **Secrecy Jurisdictions and Tax Havens**
  Countries such as the British Virgin Islands, Panama, Dubai, and Cyprus provide havens for opaque financial structures. Weak disclosure norms obscure ultimate beneficial ownership, enabling round-tripping, where illicit funds leave India and re-enter as "legitimate" foreign investment.
- **Delayed Mutual Legal Assistance Responses**
  India has signed over 45 Mutual Legal Assistance Treaties (MLATs), but responses from foreign states are often delayed for months, sometimes over a year. Bureaucracy, sovereignty

sensitivities, and the absence of binding deadlines cripple asset recovery. In the *Nirav Modi case*, UK cooperation took months, illustrating this structural handicap.

- **Uncooperative or Hostile Jurisdictions**
  States accused of sponsoring terrorism—most notably Pakistan—routinely deny links to designated terror entities, block extradition requests, and resist asset freezes. Even friendly nations sometimes hesitate, citing economic interests or political pressure.
- **Non-Harmonised Legal Definitions**
  India's frameworks (PMLA, UAPA) differ from US laws such as the Patriot Act or the UK's Proceeds of Crime Act. Divergent definitions of laundering and terror finance complicate joint prosecutions and weaken coordination.
- **Cryptocurrency Grey Zones**
  Many platforms such as Binance or KuCoin are domiciled in lightly regulated jurisdictions. Non-compliance with FATF's "Travel Rule" leaves transactions anonymous and outside India's jurisdiction, allowing laundering and terror finance via digital assets.
- **Lack of Global Consensus on Regulation**
  FATF provides standards, but no global enforcement authority exists. Geopolitical rivalries—for instance, US–China or Russia–EU tensions—stall consensus. This leaves significant gaps for illicit networks to exploit.

e. Strengthening India's Global Financial and Cyber Posture: The Way Forward

To move from compliance to leadership, India must adopt coordinated reforms that integrate diplomacy, law, and technology.

- **Modernise Domestic Frameworks**
  Extend AML coverage to decentralised finance (DeFi), online gaming, and e-wallets. Mandate real-time suspicious transaction reporting from fintech start-ups, crowdfunding platforms, and foreign payment gateways. Sector-specific guidelines for real estate, NGOs, and casinos can close persistent loopholes.
- **Fast-Track MLAT Mechanisms**
  Negotiate bilateral "digital MLATs" with strict response timelines. Use G20, BRICS, and Quad to push for global consensus on fintech regulation and time-bound cooperation treaties.
- **Build Crypto Surveillance Infrastructure**
  Establish a national blockchain analytics cell under FIU-IND/ED to trace wallets, analyse transaction patterns, and monitor smart contracts in real time. Partnering with global analytics firms (e.g., Chainalysis, TRM Labs) can accelerate this capacity.
- **Enhance Data-Sharing with Allies**
  Institutionalise secure intelligence-sharing with the UAE, Singapore, and UK. Use the Asia/Pacific Group for joint typology studies and early warning systems.
- **Champion the Global South Perspective**
  India is uniquely placed to bridge developed and developing nations. It should advocate for capacity-building grants, technology transfer, and regulatory equity through UNODC, IMF, and FATF, positioning itself as a leader of digital fairness.
- **Ensure Domestic Political Transparency**
  Global credibility starts at home. India should legislate real-time disclosure of electoral bond contributions, ban anonymous donations above a threshold, and rigorously audit NGO funding, especially where politically exposed persons (PEPs) are involved.

Conclusion

India is transitioning from a reactive AML/CFT player to a potential global norm-setter. Yet secrecy havens, MLAT delays, crypto grey zones, and definitional mismatches show that seizures and raids alone cannot resolve the problem.

Global Financial Integrity estimates that India lost nearly $88 billion annually between 2008 and 2017 through illicit outflows—mostly via trade misinvoicing and offshore structures. As one analyst

remarked: *"India's war on money laundering won't be won by raids alone—it requires global coalitions, fintech diplomacy, and legal foresight."*

By aligning domestic reforms with multilateral leadership, India can insulate its financial system while serving as a credible bridge between the Global South and global AML governance.

The discussion of money laundering and terror financing reveals that illicit finance is the bloodstream of criminal and extremist ecosystems. Dirty money fuels narcotics, arms trafficking, terror logistics, and political corruption. Yet finance is only one layer of this underground economy. Beneath it lies a deeper nexus where organised crime syndicates and terrorist groups converge, sharing routes, resources, and strategies.

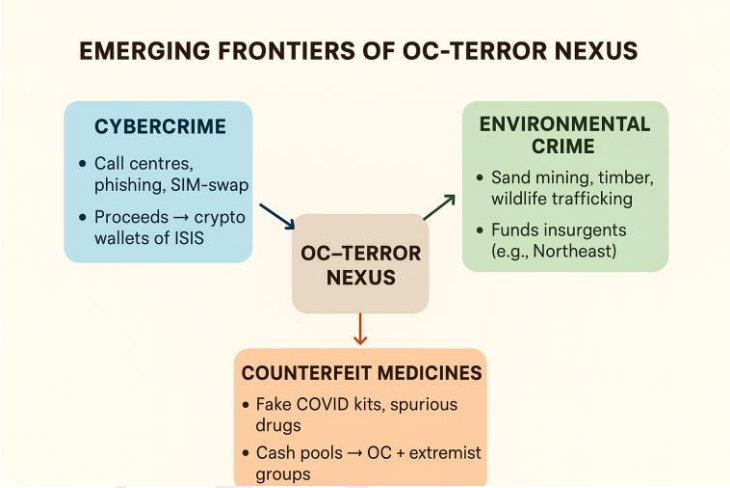
From the Dawood Ibrahim network's dual role in smuggling and terror funding, to narco-terror linkages in Punjab, to Maoist reliance on extortion cartels—the contours of India's internal security are increasingly shaped by this crime–terror fusion.

It is against this backdrop that the next chapter turns to Organised Crime and Terror Linkages, examining how gangs, mafias, and illicit economies act as both enablers and partners of extremist violence.

Chapter 8. Organised Crime and Terror Linkages

8.1 Organised Crime–Terrorism Nexus

a. Introduction



Historically, organised crime and terrorism were regarded as separate domains: the former driven by profit, the latter by ideology. In the twenty-first century, however, globalisation, porous borders, digital finance, and governance deficits have eroded this distinction. What has emerged is a symbiotic ecosystem in which crime fuels terror and terror protects crime. This relationship—termed the *"Drugs–Guns–Cash–Terror Continuum"*—has become one of the gravest threats to internal security.

For India, the vulnerabilities are particularly acute. Hostile neighbours, transnational cartels, porous borderlands in Punjab, Jammu and Kashmir, and the Northeast, along with socio-economic stresses such as youth unemployment and rural poverty, create fertile ground for this nexus. The technological enablers of encrypted messaging, cryptocurrencies, and the dark web further complicate enforcement.

The United Nations Office on Drugs and Crime (2018) warned that *"crime–terror alliances accelerate state destabilisation."* India's own experience—from the 1993 Mumbai blasts masterminded by Dawood Ibrahim's syndicate to the rise of narco-terrorism in Punjab—confirms the gravity of this threat. As one analyst put it: *"Terror needs ideology; crime needs profit. But when they converge, the result is a destabilised state."*

b. Nature of the Organised Crime–Terrorism Nexus

- **Functional Overlap**
  Organised crime networks provide terrorists with logistical infrastructure—safe houses, forged documents, vehicles, and weapons. In exchange, crime syndicates enjoy reduced law enforcement scrutiny, protection in conflict zones, and access to insurgent-controlled smuggling routes.
  Example: In Kashmir, narcotics smugglers have facilitated cross-border movement for Jaish-e-Mohammed operatives under ISI protection.
- **Resource Sharing**
  Both groups exploit overlapping underground systems for transportation, financial movement, and communication. Hawala agents, shell firms, and crypto wallets serve both criminals and extremists.
  Example: A Dubai-based hawala operator may channel funds simultaneously for a Khalistani extremist, a gold smuggler, and a cyber-fraud racket.
- **Territorial Coincidence**
  Crime and terror outfits often operate in the same weak-governance geographies—borderlands in Punjab and J&K, insurgency-hit Northeast, or urban slums in Delhi, Mumbai, and Uttar Pradesh. Alienated and unemployed youth in these areas are particularly vulnerable to recruitment by gangs and extremist organisations.
- **Mutual Benefit**
  The nexus is symbiotic rather than hierarchical. Terrorists gain anonymity and logistics from

criminal networks, while criminals benefit from ideological camouflage and entry into higher-value trafficking.
Example: In Punjab, gangsters like Arsh Dalla and Goldy Brar run extortion rackets while simultaneously pushing pro-Khalistan propaganda and conducting targeted killings under foreign instructions.

- **Proxy Conduits**
  Both crime and terror domains use front organisations—NGOs, real estate firms, or religious charities—that appear legitimate but conceal illicit operations.
  Example: In Kashmir and Kerala, banned groups have floated orphan-care trusts to secure foreign donations that are then diverted into radicalisation campaigns.

c. Why the Nexus Is Difficult to Dismantle

- **Blurred Roles of Individuals**
  The line between gangster, propagandist, and terror courier is fluid. Figures like Lawrence Bishnoi and Goldy Brar epitomise this interchangeability, making profiling and pre-emptive policing immensely difficult.
- **Digital Camouflage**
  Encrypted apps, dark web forums, and crypto mixers obscure trails. Handlers abroad can remotely control gangs inside India without ever setting foot in the country.
- **Diaspora Funding with Dual Faces**
  Diaspora contributions blur the distinction between legitimate charity and covert radical financing. Some overseas gurdwaras have been flagged for funnelling funds to Khalistani outfits.
- **Political–Police–Criminal Nexus**
  Political patronage shields criminals who double as terror facilitators, while overburdened or complicit police look away, creating pockets of impunity.
- **Legal Fragmentation**
  Crime and terror are prosecuted under separate statutes—UAPA, PMLA, IPC—resulting in turf wars between agencies, inconsistent prosecutions, and poor conviction rates.

Disrupting this nexus is thus not only a law enforcement challenge but a governance test of integration, intelligence, and institutional courage.

d. Why This Nexus Is a Grave Internal Security Concern

- **Destabilises Governance**
  Crime–terror networks establish parallel authority structures in border villages and urban slums, steadily eroding state legitimacy.
- **Erodes Rule of Law**
  Witness intimidation, corruption, and political pressure paralyse prosecutions, as seen in D-Company cases.
- **Amplifies Radicalisation**
  Organised crime syndicates fund digital propaganda, recruit from prisons, and glamorise gang culture through YouTube and social media.
- **Corrupts Institutions from Within**
  Border guards, jail staff, and local officials are bribed or coerced, enabling smuggling networks and radicalisation to persist unchecked.
- **Makes Terror Self-Sufficient**
  By tapping into organised crime revenues, terror outfits no longer depend exclusively on state sponsors—complicating attribution and deterrence.

Conclusion

The organised crime–terrorism nexus is more than a policing problem—it is a systemic threat to sovereignty, governance, and social cohesion. By merging the efficiency of criminal enterprise with the

ideological fervour of terrorism, it creates a shadow economy that is resilient, adaptive, and transnational.

Breaking this chain requires:

- Integrated intelligence fusion centres,
- A unified legal framework bridging UAPA, PMLA, and state-level anti-crime laws,
- Financial disruption of hawala, crypto, and offshore hubs,
- Modernisation of border and coastal security, and
- Global partnerships through FATF, INTERPOL, and UNODC.

As Kofi Annan cautioned: *"Organised crime and terrorism feed off each other in a mutually reinforcing cycle of violence, corruption and fear. Breaking this cycle is essential for peace and security."*

India's challenge is therefore not merely to police the nexus but to dismantle it decisively, with political will, institutional synergy, and sustained global cooperation.

The conceptual mapping of this continuum highlights how criminal profits and extremist agendas fuse into a reinforcing cycle. Yet theory alone does not capture its gravity. The real scale is revealed in lived manifestations: from Dawood Ibrahim's D-Company, which converted the Mumbai underworld into a transnational terror-financing hub, to Punjab's narco-terror corridors, where drug cartels and separatist handlers collude. These case studies expose the corrosive impact of this nexus on governance, law enforcement, and social stability.

8.2 Case Studies: D-Company and Punjab Narco-Terrorism

a. Introduction

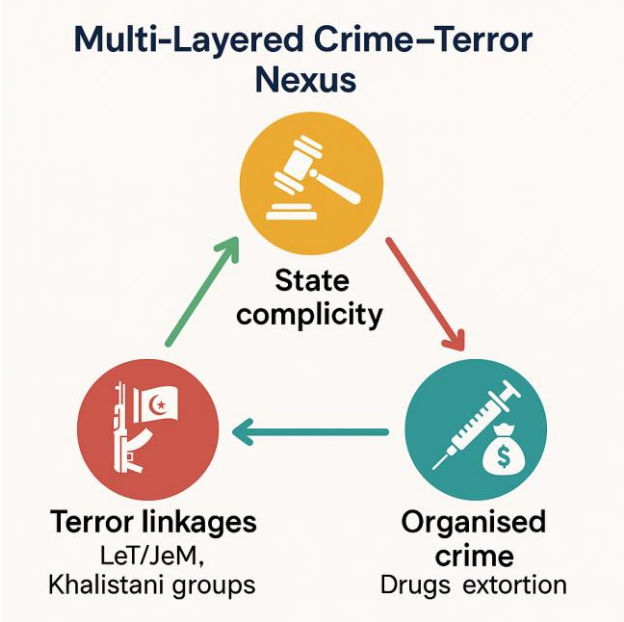
Real-world illustrations demonstrate how the crime–terror nexus mutates into hybrid threats that exploit governance loopholes, transnational linkages, and local vulnerabilities. These alliances are neither accidental nor episodic; they are systemic and adaptive, blending organised crime, radical ideology, diaspora funding, and political complicity.

i. Case Study A: D-Company – India's First Transnational Crime–Terror Enterprise

Origins in Crime
Dawood Ibrahim began as a small-time smuggler and extortionist in Mumbai's docks during the 1980s. By the decade's end, his syndicate had expanded into gold smuggling, real estate rackets, hawala channels, and cricket match-fixing.

Turn to Terrorism
The turning point came with the 1993 Mumbai bombings, which killed 257 people. The attacks, orchestrated by D-Company with financial and logistical backing from Pakistan's ISI, marked the first time an Indian crime syndicate transformed into a state-sponsored terror arm.

Transnational Reach
Today, Dawood operates primarily from Karachi under ISI protection, while investments stretch across Dubai, Pakistan,



and parts of Africa. His syndicate controls real estate, film financing, hotels, extortion rackets, and narcotics trade.

Terror Linkages
D-Company's networks have been leveraged by Lashkar-e-Taiba and Jaish-e-Mohammed, providing safe houses, logistics, and financial channels. ISI-trained operatives often shelter within its infrastructure.

Economic Footprint
With assets estimated between ₹15,000–25,000 crore, largely parked abroad, D-Company launders money through real estate and hawala systems. This makes it not merely a criminal gang but a state-backed regional security threat.

Significance
D-Company illustrates how a profit-driven syndicate can evolve into a transnational terror-financing empire when aligned with hostile state sponsorship and extremist agendas.

ii. Case Study B: Punjab Narco-Terrorism – The Drugs, Gangs, and Khalistan Triangle

Drug Corridor
Punjab sits along the Golden Crescent route, receiving heroin smuggled from Pakistan via drones, tunnels, and couriers. Drug proceeds sustain both local syndicates and cross-border handlers.

ISI's Role
Pakistan's ISI has weaponised the drug trade to finance terror modules, revive Khalistani propaganda, and recruit local gangsters. Arms and narcotics infiltration operate as twin prongs of this strategy.

Gangster–Terror Interface
Figures such as Goldy Brar and Arsh Dalla exemplify the fusion of crime with separatist ideology. Their operations span extortion, targeted killings, and propaganda at the behest of foreign handlers.

Use of Social Media and Cryptocurrency
Recruitment and propaganda flourish on Telegram and encrypted chats, while funding moves through cryptocurrency wallets and diaspora donations disguised as NGO transfers. Social media reels glorifying gangster culture double as Khalistani propaganda, drawing in disaffected youth.

Political Corruption and Weak Policing
Local complicity shields drug traffickers. Punjab's porous borders enable inflows of arms and narcotics, while prisons have become radicalisation hubs, with jailed gang leaders coordinating extortion and propaganda using smartphones.

Impact on Internal Security

- Gun culture spreads, silencing communities through extortion and terror-style killings.
- High-profile assassinations of public figures and police officers are orchestrated by gang–terror hybrids.
- Drone drops of IEDs and arms mark a new phase of cross-border warfare.
- Youth radicalisation intensifies, with drug dependency feeding both social decay and militant recruitment.

Significance
Punjab illustrates the most dangerous form of nexus—narco-terrorism—which corrodes society from within while serving the strategic aims of an external adversary.

Conclusion

Both case studies highlight how crime and terror are no longer silos. D-Company reveals how a domestic syndicate can evolve into a global terror-financing hub, while Punjab's narco-terror triangle shows how gangs, drugs, and separatist propaganda merge into a grassroots hybrid threat.

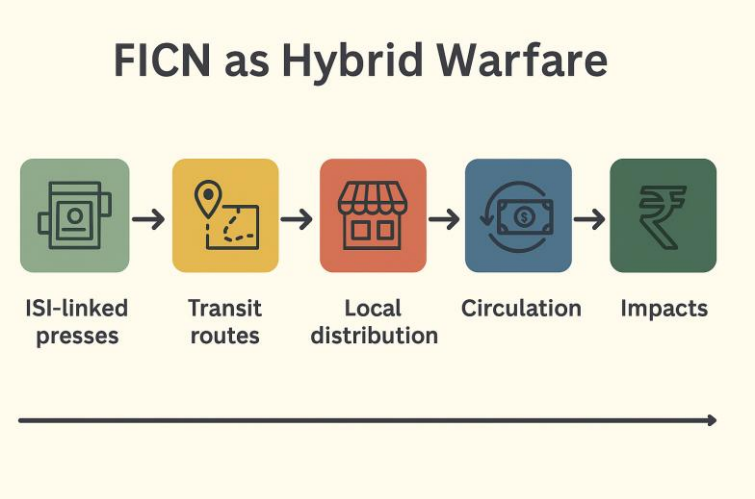
Together, they underscore that India's internal security challenge lies not only in fighting crime or terrorism separately but in dismantling their symbiosis before it consolidates into a parallel system of power.

These case studies demonstrate how illicit finance, drugs, and propaganda sustain hybrid threats. Yet one of the most insidious tools in this arsenal is not narcotics or weapons, but currency itself. Counterfeit money functions as both an economic weapon and a psychological tool—undermining markets, eroding state credibility, and funding subversion. For India, which has faced persistent attempts to flood its economy with Fake Indian Currency Notes (FICN), counterfeit networks represent a form of economic warfare directly linking organised crime, hostile intelligence agencies, and terror outfits. It is to this shadow economy of forged notes and its corrosive impact on national security that we now turn.

8.3 Counterfeit Currency Networks: Economic Sabotage as a Tool of Hybrid Warfare

a. Introduction

Counterfeit currency—especially Fake Indian Currency Notes (FICN)—is more than a financial nuisance. It has become a low-cost, deniable instrument of hybrid warfare, designed to weaken economies, corrode trust in the rupee, and fund subversion without overt conflict. This "economic sabotage by stealth" targets fiscal sovereignty, disrupts cash-dependent markets, and creates untraceable liquidity for terror and organised-crime networks.



Historically, economic sabotage via forged notes has precedents (e.g., Operation Bernhard in WWII). In the Indian context, high-quality FICN production and circulation have repeatedly been linked to transnational networks allegedly backed by hostile intelligence agencies and routed through Nepal, Bangladesh, and Gulf nodes. As a senior NIA officer observed: *"FICN is the oxygen of low-cost, deniable economic warfare—silent, persistent, and corrosive to the nation's financial architecture."*

b. Strategic Objectives Behind FICN Circulation

- **Economic Destabilisation**
    - Injecting counterfeit notes distorts monetary integrity, increases shadow liquidity, and imposes verification and replacement costs on banks and the RBI. In cash-heavy rural economies, an influx of FICN can disrupt credit cycles and market functioning (e.g., mandis).
- **Terror Financing**

- FICN provides terror groups with untraceable cash for logistics, safe houses, weapons, and recruitment—bypassing formal financial surveillance. Investigations have linked FICN to local logistics in major terror attacks.

- **Eroding Public Trust**
  - Discovery of fake notes in ATMs or banks undermines confidence in currency and monetary policy, encouraging hoarding of gold/foreign exchange and complicating future reforms (demonetisation politics being a case in point).
- **Creating Informal Power Centres**
  - Counterfeit liquidity empowers gangsters, smugglers, and insurgents as local power-brokers in border districts and prisons, often outcompeting legitimate actors.
- **Undermining Financial Inclusion**
  - Penetration of FICN in unbanked areas discourages ATM and digital adoption, weakening schemes such as Jan Dhan, DBT, and UPI.
- **Facilitating Corruption & Political Influence**
  - Forged currency surfaces during elections, funding anonymous campaign activity and bribes—thereby enabling foreign-backed groups to distort democratic processes.
- **Silent War on Sovereignty**
  - Unlike kinetic warfare, counterfeit currency corrodes economic and social stability incrementally—akin to a persistent, low-cost campaign that weakens state authority and public confidence.

c. Cross-Border FICN Ecosystem

- **Pakistan**: Widely identified as the epicentre—alleged state-linked presses have produced high-grade FICN that reach India via multiple routes.
- **Bangladesh & Nepal**: Act as transit corridors; towns bordering India (e.g., Malda, Raxaul, Birganj) are documented hubs for inflows and onward distribution.
- **UAE & Gulf**: Dubai and other Gulf nodes function as staging posts; couriers and hawala operators often coordinate bulk consignments.
- **Local Indian Nodes**: Malda, Kishanganj and similar towns serve as distribution and circulation points; low-income labourers are recruited as unwitting carriers.

This transnational chain links production (secure presses), transit (corridor logistics), and distribution (local markets, prisons, elections), forming an adaptive network that re-emerges after countermeasures (e.g., post-2016 demonetisation resurgence by 2020–21).

d. Modus Operandi of Networks

Counterfeit networks operate like sophisticated supply chains:

- **Production** — High-grade printing using near-state presses, special inks, and paper that mimic genuine notes.
- **Transit** — Smuggling via land borders, concealed trade consignments, courier routes, or diplomatic/merchant cover.
- **Distribution** — Mixed into genuine bundles and circulated through rural markets, prisons, labour contractors, and election channels.
- **Integration** — Linked operationally to hawala, narcotics, and arms trafficking, sharing logistics, personnel, and concealment techniques to lower detection risk.

e. Technical Aspects of FICN Circulation

The resilience of counterfeit networks lies in their ability to match state-grade technology with adaptive distribution. Over the years, the quality, denominations, and circulation methods of Fake

Indian Currency Notes (FICN) have grown increasingly sophisticated, making detection a formidable challenge for Indian authorities.

- **Quality of Fake Notes**
    - State-sponsored presses, particularly in Pakistan, have replicated 8–10 of the 17 RBI security features, including watermarks, latent images, see-through registration marks, colour-shifting inks, and micro-lettering.
    - Although demonetisation (2016) disrupted supply chains, counterfeiters adapted rapidly. Redesigned ₹500 notes have already appeared with partial replication of optically variable inks and tactile features, making some fakes nearly indistinguishable from genuine notes.
- **Denominations Targeted**
    - Historically: ₹500 and ₹1000 (later ₹2000) were preferred for high-value laundering.
    - Post-demonetisation: counterfeiters shifted focus to:
        - ₹500 notes – India's most circulated high-value denomination.
        - ₹100 and ₹200 notes – dominant in rural markets, less scrutinised, ideal for stealth diffusion.
    - Smaller denominations blend easily into daily transactions and evade suspicion.
- **Printing Techniques Used**
    - Offset printing, high-resolution scanning, and AI-based image enhancement.
    - Replication of UV inks and sophisticated microprinting techniques.
    - Reports suggest Pakistan-based presses import specialised inks and paper to mimic RBI-grade security threads.
    - Emerging threats: 3D printing and nanotechnology inks, which could revolutionise counterfeiting.
- **Distribution Mechanisms**
    - **Transit Routes**: Nepal and Bangladesh borders remain the main entry points.
    - **Couriers**: Women, minors, and low-profile carriers.
    - **Parcel Services**: Fake Aadhaar IDs and untraceable drop-off points exploited.
    - **Rail/Road Networks**: Flow into cash-heavy markets such as mandis, festivals, and election rallies.
    - **Retail Laundering**: Introduced via fuel stations, dhabas, donation boxes, and small vendors.
    - Frequently mixed with genuine bundles to bypass casual checks.
- **Layered Introduction Strategy**
    - Instead of mass flooding, FICN is released in small, staggered volumes across regions.
    - This avoids statistical anomalies in RBI's detection systems and keeps law enforcement tied up in fragmented seizures, masking central coordination.
- **Link to Other Illicit Networks**
    - FICN supply chains are integrated with hawala, narcotics, arms smuggling, and terror logistics.
    - Shared couriers and digital handlers create a "multi-commodity smuggling model," lowering costs and improving concealment.

f. Institutional Response

India has deployed multiple agencies to tackle the counterfeit menace, though challenges of sophistication, scale, and coordination persist.

- **National Investigation Agency (NIA)**

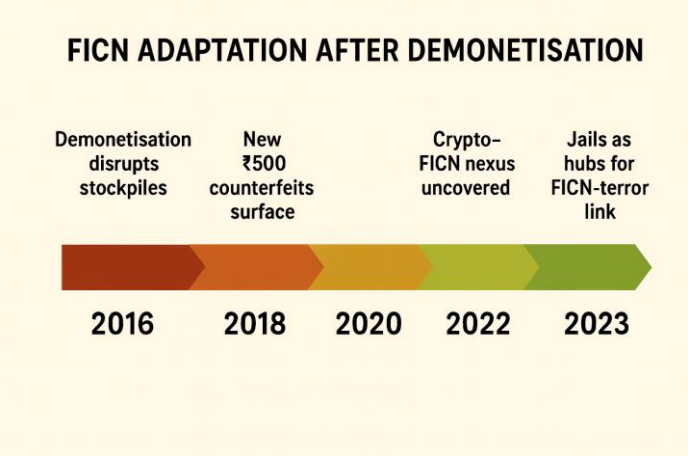
- Handles FICN cases linked to terrorism, prosecuting under the UAPA alongside provisions of the Bharatiya Nyaya Sanhita (BNS).

- **Reserve Bank of India (RBI) and Banks**
  - Issue guidelines, conduct staff training, and publish monthly seizure data.
  - Regularly upgrade note features and verification systems.
- **Directorate of Revenue Intelligence (DRI) and Customs**
  - Intercept counterfeit consignments at airports, seaports, and land borders.
  - Known for bulk seizures and disruption of high-value smuggling channels.
- **State ATS and Police Forces**
  - Manage ground-level seizures and arrests, especially in hubs such as Malda (West Bengal), Mumbai, and Hyderabad.
  - Work closely with central agencies but remain uneven in capacity and technical expertise.

Despite these measures, enforcement remains fragmented. The integration of counterfeit flows with narcotics, hawala, and arms trafficking means even large seizures represent only the visible tip of the iceberg. As one analyst noted, *"Every fake note seized is not a victory, but a symptom of a much deeper penetration."*

g. Persistent Challenges in Tackling FICN

Despite multiple institutional efforts, India continues to face deep-rooted hurdles that undermine its anti-FICN strategy:



- **Border Porosity**
  - India's long frontiers—1,751 km with Nepal and 4,096 km with Bangladesh—remain porous, unfenced, or riverine.
  - Smugglers exploit trails, forests, and rivers, aided by ethnic overlaps and local sympathies.
  - *Example*: Malda (West Bengal) and Raxaul (Bihar) persist as notorious gateways.
- **Technological Adaptation by Counterfeiters**
  - State-sponsored presses employ offset lithography, 3D replication, UV ink duplication, and AI-based imaging.
  - Emerging risk: deep learning–generated synthetic replicas, capable of near-perfect forgery.
- **Inadequate Prosecution and Low Conviction**
  - Despite FICN being cognisable and non-bailable, cases collapse due to:
    - shortage of forensic experts,
    - weak chain-of-custody,
    - duplication of charges,
    - witness non-appearance.
  - Result: acquittals or trials dragging for years, eroding deterrence.
- **Misuse of Legal Currency Channels**
  - Fake notes laundered through petrol pumps, toll plazas, mandis, and religious donations.

- Cooperative banks and SHGs with weak KYC norms ease their integration.
- Bundling with genuine notes below reporting thresholds ensures stealthy deposits.

- **Weak Inter-Agency Coordination**
  - NIA, ED, DRI, RBI, and state police often work in silos.
  - Lack of a unified FICN database prevents linking seizures to terror financing trails.
- **Digital–Physical Laundering Convergence**
  - Fake notes exchanged for cryptocurrency at discounts.
  - Proceeds reinvested in local businesses or campaign donations.
  - Investigations (Kerala, Maharashtra 2022–23) exposed crypto–FICN nexuses.

h. Recent Trends in FICN Circulation (Post-2016)

- **Post-Demonetisation Recovery**
  - 2016 demonetisation disrupted counterfeit pipelines.
  - By 2019, Pakistan-backed presses had adapted to redesigned ₹500 notes.
- **Shift to Lower Denominations**
  - ₹500 still dominates, but counterfeiters increasingly target ₹100 and ₹200 notes, especially in rural and informal markets.
- **Crypto–FICN Nexus**
  - Darknet forums and P2P exchanges enable trading of fake notes for crypto, bypassing AML frameworks.
- **Regional Hotspots**
  - **Uttar Pradesh**: Indo–Nepal corridor.
  - **West Bengal**: Malda as a critical hub.
  - **Maharashtra**: Financial hubs and slums.
  - **Kerala**: Gulf diaspora + hawala + crypto channels.
- **Direct Terror Financing Links**
  - Seizures in J&K and Kerala tied counterfeit notes to logistics for Pulwama and Udaipur attacks.
- **Prisons as Hubs**
  - Corrupt wardens and inmates facilitate FICN circulation.
  - Radical elements recruit smugglers inside jails, creating closed-loop ecosystems.

Conclusion

The counterfeit currency threat is not about forgery alone—it is a calculated hybrid warfare strategy. Each forged note undermines sovereignty, destabilises the economy, and empowers crime-terror networks.

- For adversaries: FICN is cheap, deniable, and scalable.
- For India: the costs are economic distortion, terror financing, reputational harm, and enforcement fatigue.

Breaking this chain demands:

- A national FICN intelligence database linking RBI, NIA, ED, DRI, and state police inputs.
- AI-resistant security features such as nanotech inks and blockchain-enabled serial verification.
- Hardened borders along Indo–Nepal and Indo–Bangladesh corridors with community intelligence.

- Targeted disruption of hawala, crypto, and political finance pipelines.
- Global cooperation via FATF, INTERPOL, and regional task forces to choke supply at source.

RBI's 2022–23 report confirmed over 9 lakh counterfeit notes detected, mostly in ₹500 denomination—a number that represents only the visible tip of a larger shadow economy.

As Raghuram Rajan warned: *"A nation's currency is a symbol of its sovereignty. To attack it is to attack the very idea of the nation."*

Thus, India must treat FICN not as a niche financial crime but as an instrument of hybrid warfare, demanding the same urgency as a territorial or armed incursion.

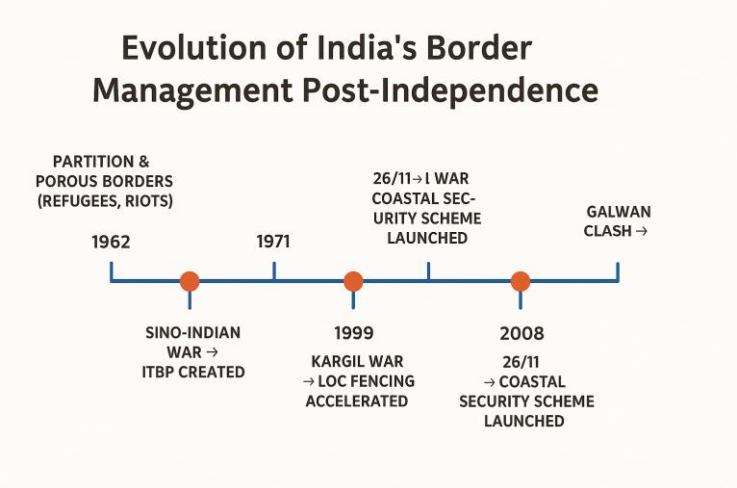
The interplay of organised crime, narco-terrorism, counterfeit currency, and arms smuggling reveals a common denominator: porous borders. Whether it is heroin infiltrating Punjab, fake notes in Malda, or weapons through Myanmar, India's security repeatedly hinges on border vulnerabilities. Effective border management is therefore not just about sovereignty, but the first line of defence against hybrid threats.

It is this critical dimension that the next chapter explores in detail—India's border management framework, challenges, and reforms.

Chapter 9. Border Management in India: Concepts, Challenges & Institutions

9.1 Understanding Border Management in India

a. Introduction



Border management is best understood as a multidimensional process that balances security, regulation, and cooperation. It is not confined to fencing or patrolling alone but extends to monitoring the flow of people, goods, and information, while also enabling legitimate cross-border trade, transit, and regional development.

In India, border management is uniquely complex. Geographically, the country spans Himalayan ranges, deserts, dense forests, riverine belts, and 7,500+ km of coastline. Geopolitically, it contends with both hostile and sensitive neighbours—Pakistan, China, and Myanmar on the one hand, and culturally overlapping partners such as Nepal, Bhutan, and Bangladesh on the other. Many of India's insurgency-prone regions—Jammu and Kashmir, Nagaland, and Manipur—sit astride these borders, amplifying their volatility.

In the age of hybrid threats, vulnerabilities are no longer limited to infiltration or smuggling. Drone-based narcotics drops, cyber intrusions from across frontiers, and psychological warfare in border communities illustrate how traditional boundaries now intersect with new-age challenges.

As one strategist observed: *"Borders are not just lines of defence—they are dynamic spaces where national security, foreign policy, local governance, and human lives intersect."* This perspective underscores why India's border management must combine fortification, intelligence coordination, diplomacy, trade facilitation, and community development.

b. Types of Borders in India

- **Line of Control (LoC)**
  - De facto boundary between India and Pakistan in Jammu & Kashmir.
  - Among the most militarised frontiers globally, marked by infiltration, cross-border shelling, and ceasefire violations.
  - Guarded by the Indian Army and the Border Security Force (BSF).
- **Line of Actual Control (LAC)**
  - Stretches 3,488 km between India and China.
  - Undefined in many sectors, resulting in patrolling face-offs, salami-slicing tactics, and infrastructure competition.
  - Guarded by the Indian Army and the Indo-Tibetan Border Police (ITBP).
- **International Borders (IB)**
  - Officially recognised boundaries with Pakistan, Bangladesh, Myanmar, Bhutan, and Nepal.
  - Managed by different agencies: BSF (western & eastern), SSB (Nepal & Bhutan), and Assam Rifles (Myanmar).
- **Riverine Borders**

- Found in West Bengal, Assam, and Bihar.
- Highly porous due to shifting channels and difficulty of fencing.
- Hotspots for illegal migration, cattle smuggling, and contraband trade.

- **Open Borders**
  - By treaty, India maintains visa-free movement with Nepal and Bhutan.
  - While facilitating cultural and economic ties, they are often misused for fake identity creation, cross-border crime, and terror financing.
- **Coastal Borders**
  - India's 7,516 km coastline spans nine states and four UTs.
  - Includes critical infrastructure—ports, refineries, and naval bases—but also vulnerable fishing hamlets.
  - The 26/11 Mumbai attack exposed how sea routes can be exploited.
  - Secured by the Indian Navy, Coast Guard, and Marine Police.

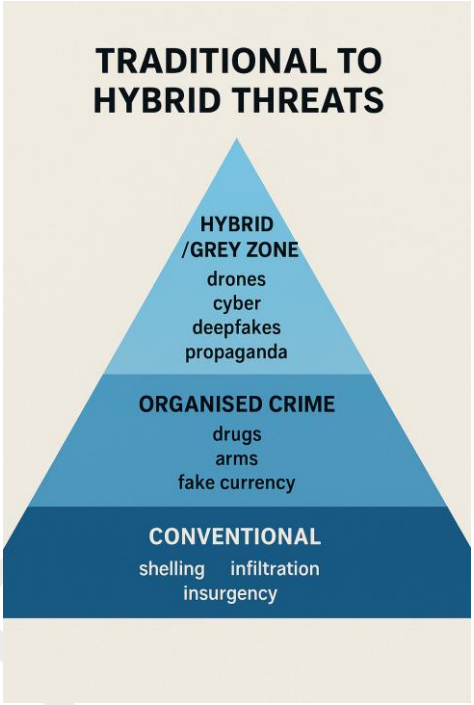
c. Why Border Management is Critical for India

- **Two-Front Security Threat**
  - Pakistan front defined by proxy war and infiltration.
  - China front marked by infrastructure races and stand-offs.
  - Together, they create a unique two-front challenge.
- **Gateway for Terrorism and Organised Crime**
  - Borders serve as entry points for terrorists, drug traffickers, counterfeiters, and arms smugglers.
  - Porous stretches in Nepal, Bangladesh, and Myanmar are particularly vulnerable.
- **Internal Security Spillover**
  - Conflict-prone states (e.g., J&K, Manipur) rely on porous borders for insurgent sanctuary and regrouping.
- **Border Populations as First Responders**
  - Frontier communities act as eyes and ears of the state.
  - Neglect risks alienation, propaganda vulnerability, and recruitment by criminal/terror networks.
- **Protection of Strategic Assets**
  - Border zones host highways, dams, refineries, and defence infrastructure—prime sabotage targets.
- **Trans-border Cultural Overlaps**
  - Shared ethnic ties (e.g., Naga tribes across India–Myanmar) create both cultural bridges and law enforcement challenges.
- **Coastal and Riverine Vulnerability**
  - Difficult-to-secure zones enable narco-landings, illegal migration, and smuggling.
  - The 26/11 infiltration remains the starkest warning.
- **Hybrid Threats and Grey-Zone Warfare**
  - Drone-dropped arms, Chinese information ops, and cross-border cyber attacks redefine border threats.
- **Diplomatic Fallout**
  - Border incidents escalate into international crises, impacting India's diplomatic leverage (e.g., Galwan 2020).
- **Development Imperative**

- Infrastructure, healthcare, and jobs in frontier regions act as strategic stabilisers.
- Developmental neglect fosters alienation and outmigration.

Conclusion

Border management in India is far more than military fortification—it is about creating a secure, stable, and integrated frontier. In the age of hybrid warfare—where drones, disinformation, and illicit flows blur war and peace—borders represent both the first shield of sovereignty and the final bridge of integration.



As the *Arthashastra* reminds us: *"A king who neglects the borders will find his sovereignty negotiated at another's table."* Today, with over 60% of India's borders cutting through difficult terrain, technology, infrastructure, and community participation form the indispensable triad of lasting security.

The conceptual framework highlights why India's borders are simultaneously spaces of opportunity and vulnerability. But challenges are not uniform—each frontier has its own character:

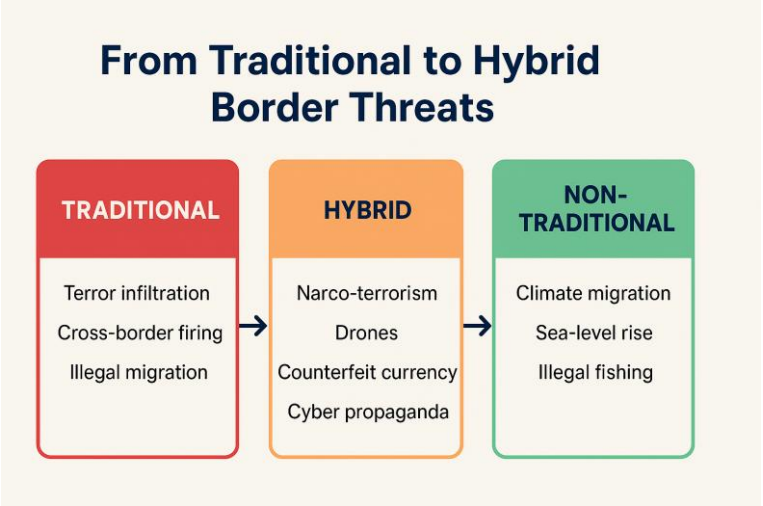
- The LoC is dominated by infiltration and proxy war.
- The LAC is defined by salami-slicing and infrastructure races.
- The Bangladesh border struggles with illegal migration and smuggling.
- Riverine and coastal frontiers face narco-terror and maritime infiltration.

To grasp the full magnitude of India's security dilemma, the next section turns to a sector-wise mapping of border challenges, tracing how geography, neighbour-specific hostility, and demographic pressures shape the country's border management landscape.

9.2 Sector-wise Issues in India's Borders

a. Introduction

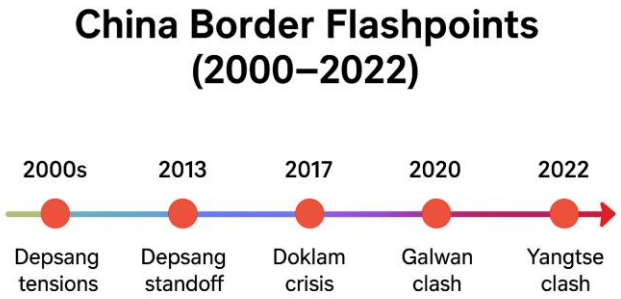
India's geography has gifted it both opportunity and vulnerability: 15,106 km of land borders with seven countries and 7,516 km of coastline. Yet these frontiers are not uniform. Each sector reflects its own mix of terrain, demography, historical baggage, and threat matrix. Border management, therefore, cannot follow a single model—it must be sector-specific, blending military vigilance with governance, diplomacy, and community development.



The spectrum of risks stretches from high-altitude flashpoints with China to porous migration corridors with Bangladesh, and from narco-terror pipelines in Punjab to sea-borne infiltration in Mumbai and Gujarat. Hybrid threats—counterfeit currency, drones, and cyber-enabled propaganda—have further blurred the lines between traditional and non-kinetic warfare.

According to the Ministry of Home Affairs (2023):

- Over 4,000 infiltration attempts were detected along the western border in the past decade.
- More than 1.4 lakh illegal migrants were apprehended on the eastern frontier in just five years.



These figures underscore that border management in India is as much about governance and diplomacy as about military defence. As Shivshankar Menon observed:
"Borders are not just lines on maps—they are lines of trust, strength, and resilience. Lose control of them, and you begin to lose control of the state itself."

i. Western Sector – India–Pakistan Border (J&K, Punjab, Rajasthan, Gujarat)

The western frontier is India's frontline against a hostile neighbour, where conventional hostility converges with asymmetric tactics.

- **Terror Infiltration**: Lashkar-e-Taiba and Jaish-e-Mohammed militants attempt frequent crossings, often timed with elections or festivals.
- **Launch Pads & Camps**: Over 40 terror camps operate in Pakistan-occupied Kashmir under ISI patronage.
- **Tunnel Intrusions**: Multiple cross-border tunnels have been unearthed, used for militants, narcotics, and arms.
- **Drone Drops**: Since 2019, drones have been used to deliver weapons, heroin, and IEDs across Punjab and J&K.
- **Narco-Terror & FICN**: Heroin consignments and counterfeit notes infiltrate via Punjab and Gujarat, financing crime-terror networks.

Here, kinetic warfare (guns & shells) converges with hybrid tactics (tunnels, drones, Telegram propaganda), making it India's most volatile frontier.

ii. Eastern Sector – India–Bangladesh and Myanmar Borders

The eastern frontier is marked by migration, smuggling, and ethnic spillovers.

- **Illegal Migration**: Persistent flows from Bangladesh into West Bengal and Assam trigger demographic stress and communal friction, intensified by NRC–CAA politics.
- **Cattle & Goods Smuggling**: Smuggling of cattle, narcotics, and counterfeit consumer goods thrives in Bengal's porous zones.
- **Ethnic Spillover (Myanmar)**: Chin, Kachin, and Rohingya unrest spills into Manipur and Mizoram, complicating refugee and security policies.
- **Insurgent Hideouts**: ULFA-I and NSCN-K exploit Myanmar's jungles as safe havens.
- **Challenging Terrain**: Forests and riverine belts hinder fencing and surveillance, straining BSF and Assam Rifles.

Here, poverty, politics, and porous terrain converge—making smuggling a livelihood and insurgency a legacy.

iii. Northern Sector – India–China Border (LAC: Ladakh, Uttarakhand, Himachal, Arunachal)

The northern frontier is dominated by strategic contestation and grey-zone warfare.

- **Salami Slicing**: PLA alters ground realities incrementally through patrol intrusions and village-building.
- **Infrastructure Race**: China's all-weather roads and model villages contrast with India's slower BRO-led projects (though DS-DBO Road and Atal Tunnel mark progress).
- **Flashpoints**: Doklam (2017) and Galwan (2020) reveal the sector's volatility.
- **Ambiguity of LAC**: Differing perceptions fuel routine face-offs.
- **High-Altitude Risks**: Any escalation requires troops to endure extreme cold, thin air, and logistical strain.

Here, the contest is not only for territory, but also for maps, narratives, and psychological dominance.

iv. Northeastern Sector – Borders with Myanmar, Bhutan, and Bangladesh

This region is both a corridor of connectivity and a crucible of insurgency.

- **Insurgency & Arms Flow**: ULFA, NSCN, and PLA groups exploit safe havens across Myanmar and Bangladesh.
- **Free Movement Regime (FMR)**: The 16 km visa-free regime along the India–Myanmar border aids cultural ties but is misused by insurgents and smugglers.
- **Cross-Border Kinship**: Shared ethnicities hinder intelligence penetration.
- **Drugs & Wildlife Trade**: The region is a hub for heroin, methamphetamine, and exotic animal trafficking.
- **Weak Infrastructure**: Poor connectivity creates vacuums exploited by insurgents.

The Northeast is India's gateway to Southeast Asia, but without trust and development, it risks being a tunnel of instability.

v. Coastal Borders – India's Maritime Frontier

The seas are India's most open yet least defended frontiers.

- **Sea-borne Terror**: The 26/11 attack highlighted glaring gaps in maritime policing.
- **Drug & Arms Landings**: Gujarat, Maharashtra, Kerala, and Tamil Nadu are frequent landing sites.
- **Surveillance Deficits**: Despite radar chains and Sagar Kavach drills, coordination among Coast Guard, Navy, Customs, and Marine Police remains patchy.
- **Illegal Fishing**: Cross-border incursions by Sri Lankan and Bangladeshi trawlers create livelihood tensions.
- **Climate Threats**: Rising seas and coastal erosion threaten Lakshadweep and Andaman–Nicobar Islands.

This sector shows how 21st-century threats float in—silent, swift, and deniable.

Conclusion

India's borders are not mere territorial markers but barometers of sovereignty and governance. Each frontier presents a distinct challenge:

- The West tests India against Pakistan's hybrid war.
- The North against China's salami-slicing tactics.
- The East & Northeast against migration and insurgency.

- The Coasts against terror, smuggling, and climate shocks.

The way forward lies in sector-specific strategies: hardened, tech-enabled frontiers in the west and north; integrated socio-economic approaches in the east and northeast; and maritime domain awareness in the seas.

As former Coast Guard DG Rajendra Singh noted: *"In the 21st century, a nation's security is measured not by the length of its borders, but by the depth of its surveillance and the reach of its governance."*

The sectoral analysis makes one fact clear: geography and geopolitics alone do not determine border vulnerability—technology and infrastructure do.

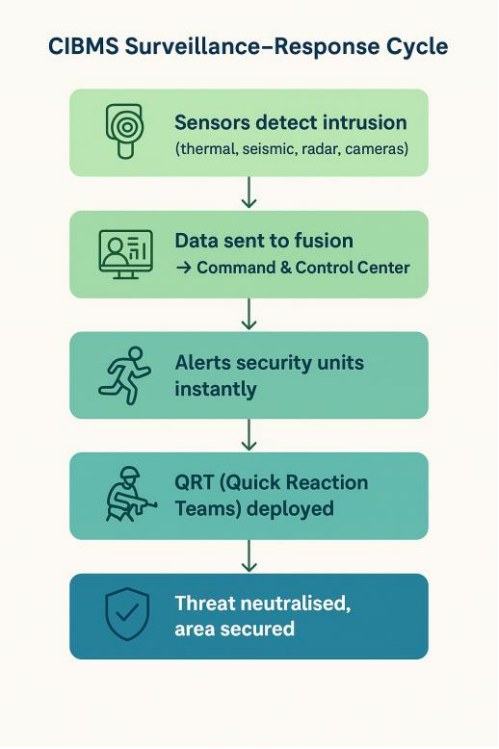
- China races ahead with all-weather roads and dual-use villages along the LAC.
- Pakistan innovates with tunnels and drones.
- Bangladesh-based smugglers exploit riverine gaps.
- The Arabian Sea tests India's maritime vigilance.

India's border agencies often remain manpower-heavy and reactive, handicapped by weak infrastructure and patchy surveillance. This brings us to the next theme: the role of infrastructure and technology in border security—where the transition from *"boots on the ground"* to *"bytes in the sky"* is no longer optional but essential.

9.3 Infrastructure and Technology for Border Security

a. Introduction

For a country like India—with more than 15,000 km of land frontiers and over 7,500 km of coastline—the task of securing borders cannot rely on manpower alone. Guarding every stretch with sentries and patrols is not only operationally unfeasible but also financially unsustainable. The immense diversity of India's borders, from the frozen heights of Ladakh to the dense forests of the Northeast, and from riverine Assam to the open waters of Gujarat and Tamil Nadu, necessitates a technology-driven and infrastructure-backed model of border management.



In the twenty-first century, border security is no longer synonymous with barbed wire and watchtowers. It revolves around networked sensors, real-time data fusion, and rapid-response capabilities. Smart infrastructure such as all-weather roads, high-altitude tunnels, and fortified forward posts, complemented by advanced surveillance systems like thermal imagers, seismic detectors, and counter-drone technology, now forms the backbone of India's frontier defence.

As former BSF Director General K. K. Sharma observed: *"Where boots cannot patrol, bytes must. Border security in the twenty-first century is as much about sensors as it is about soldiers."*

Thus, infrastructure and technology are not mere multipliers of force—they are fundamental necessities, enabling India to maintain constant vigilance, deter infiltration, and respond swiftly across some of the most inhospitable terrains in the world.

i. Smart Fencing and Electronic Surveillance Systems

India has steadily transitioned toward technology-centric surveillance through initiatives such as the Comprehensive Integrated Border Management System (CIBMS).

- **BOLD-QIT (Border Electronically Dominated Quick Response Team Interception Technique):**
  Deployed in Assam's riverine Dhubri sector, this integrates thermal imagers, infrared sensors, radars, laser fences, and fibre optics into a unified grid where fencing is not feasible.
- **Comprehensive Integrated Border Management System (CIBMS):**
  Serves as the backbone of modern surveillance, combining command-and-control centres, night-vision devices, seismic sensors, ground-based radars, and smart fencing. Piloted in Punjab and Jammu, it is gradually expanding.
- **Laser Walls:**
  Virtual barriers deployed in marshy and riverine zones of Punjab and Jammu that detect movement by laser-beam interruption, instantly alerting units.
- **Anti-Drone Technologies:**
  With rising drone-based smuggling of arms and narcotics, India is testing radio jamming, GPS spoofing, and disabling systems through DRDO, BSF, and the Air Force.

ii. Physical Infrastructure Development

Electronic systems enhance vigilance, but physical infrastructure ensures mobility, logistics, and resilience.

- **Fencing:** Over 98% of the India–Pakistan and India–Bangladesh borders are fenced. In inaccessible terrain, smart fencing is used.
- **All-Weather Roads:** BRO projects such as the DS–DBO Road (Ladakh) and Tawang routes (Arunachal Pradesh) ensure year-round troop mobility. Coastal highways bolster maritime security.
- **Foot Tracks and Ropeways:** Enable supply to remote forward posts in hilly states like Uttarakhand and Arunachal Pradesh.
- **Observation Towers and Bunkers:** Reinforced bunkers with underground shelters strengthen defences along LoC, LAC, and IB.
- **Bridges and Tunnels:** Strategic links such as the Atal Tunnel (Himachal Pradesh) and Sela Tunnel (Arunachal Pradesh) guarantee connectivity even in snowbound conditions.

iii. Coastal and Maritime Surveillance Systems

The 2008 Mumbai attacks prompted major reforms in maritime security.

- **Coastal Surveillance Radar Chain:** 46+ radars across states and islands track vessels in real time.
- **SAGAR Kavach Exercises:** Joint drills involving Navy, Coast Guard, Police, and Customs to test inter-agency readiness.
- **Automatic Identification System (AIS):** Mandates transponders on boats and ships, broadcasting ID, speed, and location.
- **NC3I Network (National Command, Control, Communication & Intelligence):** Operated from IMAC, Gurugram, integrating radar, satellite, and AIS data into a unified grid.
- **Marine Commandos (MARCOS):** Deployed at sensitive nodes and islands to counter infiltration and sabotage.

iv. Integrated Check Posts (ICPs)

Infrastructure is not just about defence—it also regulates legitimate flows of trade and people.

- **Purpose:** ICPs combine immigration, customs, warehousing, cargo scanning, foreign exchange, and quarantine facilities.
- **Management:** Operated by the Land Ports Authority of India.
- **Key ICPs:** Attari (Pakistan), Petrapole (Bangladesh), Raxaul (Nepal), and Moreh (Myanmar).
- **Benefits:** Enhance transparency, reduce corruption, improve trade efficiency, and provide systematic cross-border monitoring.

Conclusion

In the twenty-first century, technology and infrastructure are indispensable pillars of border security. From smart fencing and seismic sensors on the western frontier to radar chains and NC3I integration along the coast, these systems extend the reach of security forces far beyond human limits.

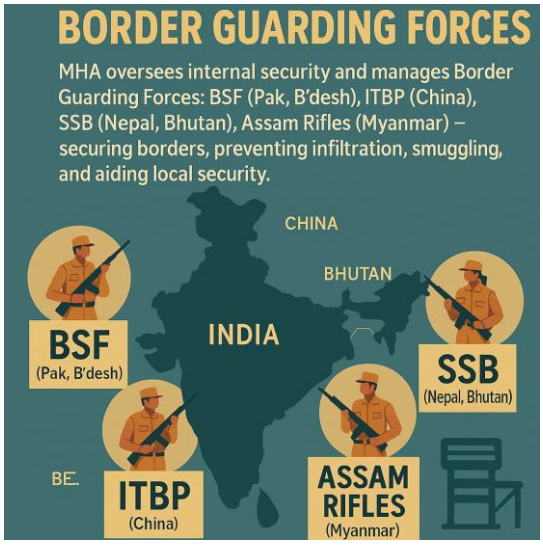
Future preparedness demands investment in AI-enabled surveillance, counter-drone capabilities, and mobility infrastructure to keep pace with adversaries' innovations. As one strategist aptly remarked: *"In the age of drones and satellites, borders are secured as much by circuits as by courage."*

While circuits, sensors, and tunnels form the backbone of border security, they are not substitutes for human presence. Roads and radars create the enabling environment, but the decisive factor remains the men and women who patrol, monitor, and respond. India's borders are guarded by a mosaic of specialised forces—from the BSF on the western front to the ITBP on the icy LAC, and the Coast Guard at sea.

Thus, having examined the infrastructure and technological foundations, we now turn to the human dimension of border management—the Border Guarding Forces of India, their mandates, deployments, challenges, and role in hybrid warfare.

9.4 Border Guarding Forces in India

a. Introduction



India's border security architecture is not guarded by a single uniform but by a mosaic of specialised forces, each adapted to the distinct terrain, threats, and geopolitical sensitivities of its sector. With over 15,000 km of land frontiers and more than 7,500 km of coastline, no single doctrine can secure all frontiers—from the icy Himalayan heights of Ladakh, to the porous riverine belts of Assam, to the open seas of Gujarat and Tamil Nadu.

These forces, drawn from both the Ministry of Home Affairs (MHA) and the Ministry of Defence (MoD), go beyond the task of guarding territory. They conduct counter-infiltration, anti-smuggling, counterinsurgency, coastal vigilance, and community outreach, making them both a shield against external threats and a bridge between the state and border populations.

As one senior BSF officer aptly remarked:
"India's borders are guarded not by one uniform, but by a mosaic of forces—each adapted to its frontier's unique demands."

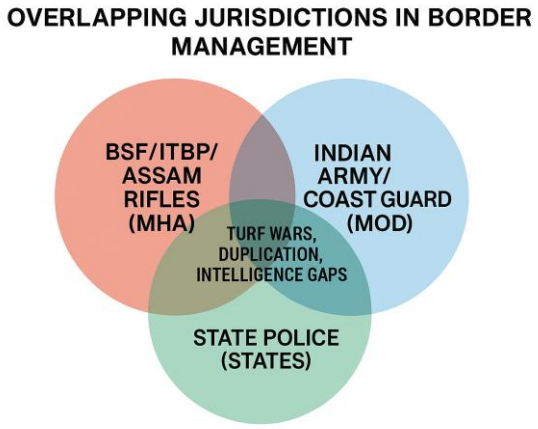
b. Overview of Key Border Guarding Forces

- **Border Security Force (BSF):**
  Under the MHA, the BSF guards the India–Pakistan and India–Bangladesh borders. It

conducts patrolling, counter-infiltration, anti-smuggling operations, and acts as the first responder during cross-border shelling or ceasefire violations.

- **Indo–Tibetan Border Police (ITBP):**
  Deployed along the Line of Actual Control (LAC) with China, across Ladakh, Himachal Pradesh, Uttarakhand, and Arunachal Pradesh. Operating in high-altitude, sub-zero conditions, the ITBP supports the Army during face-offs, undertakes surveillance, and assists in Himalayan disaster relief.
- **Sashastra Seema Bal (SSB):**
  Secures the open borders with Nepal and Bhutan, monitoring cross-border flows, countering illegal migration and human trafficking, and gathering grassroots intelligence.
- **Assam Rifles:**
  The oldest paramilitary force, it is administratively under the MHA but operationally controlled by the Army (MoD). It secures the India–Myanmar border, undertakes counterinsurgency in the Northeast, and engages in civic action programmes to build trust with local communities.
- **Indian Coast Guard (ICG):**
  Under the MoD, the ICG patrols India's 7,500 km coastline. Its responsibilities span anti-smuggling, anti-poaching, coastal security, search-and-rescue, and shipping regulation, making it the maritime counterpart of land-based border forces.
- **Indian Army:**
  The frontline combat force, deployed along the LoC with Pakistan and the LAC with China. It manages forward posts, responds to escalations, and coordinates with paramilitary forces to ensure deterrence and combat readiness.
- **Marine and Coastal Police:**
  Functioning under state governments, they monitor fishing vessels, ports, and coastal villages. Their role is micro-level coastal policing, preventing infiltration, smuggling, and illegal fishing, thereby complementing the Navy and Coast Guard.

c. Major Challenges Faced by Border Guarding Forces



- **Harsh Terrain and Climatic Extremes**
  Forces contend with some of the world's toughest environments—from ITBP and Army posts at 15,000+ feet in minus 40°C temperatures, to Assam Rifles battling dense forests and monsoons, to BSF jawans enduring Rajasthan's desert heat. These conditions strain both manpower and logistics.
- **Manpower Fatigue and Mental Stress**
  Long stretches of isolation, minimal leave, and relentless vigilance lead to fatigue, depression, and even suicides. Incidents of fratricide and public complaints (such as BSF jawans' viral videos in 2017) reflect deeper morale concerns.
- **Infrastructure Deficits in Forward Posts**
  Many outposts lack all-weather connectivity, helipads, modern bunkers, power, or sanitation. In regions like Ladakh and Arunachal Pradesh, reaching posts can take days of trekking, complicating both supply and emergency evacuation.
- **Technology Gaps and Uneven Modernisation**
  While Punjab and J&K benefit from smart fencing and CIBMS, other sectors rely almost entirely on foot patrols. Anti-drone systems, AI-enabled surveillance, and night-vision devices remain unevenly deployed.

- **Overlapping Jurisdictions and Coordination Issues**
  With multiple forces operating without a unified command, duplication of effort and intelligence delays are common. Examples include BSF–state police friction in Punjab or Coast Guard–Marine Police overlaps. The dual control of Assam Rifles (MHA & MoD) also creates operational ambiguity.
- **Resource Constraints and Logistical Delays**
  Procurement of critical equipment—winter gear, UAVs, radars—often faces delays due to funding bottlenecks and complex tendering procedures, weakening operational readiness.
- **Inadequate Training for Hybrid Threats**
  Border forces face drones carrying explosives, biometric spoofing, cyber intrusions, and encrypted communications, yet training still emphasises conventional tactics with limited adaptation to digital-age threats.
- **Political and Legal Sensitivities**
  Operations in Nagaland, Manipur, and Kashmir are fraught with sensitivities, where missteps can spark civilian backlash, international criticism, or renewed insurgency—making border duties as much political and psychological as tactical.
- **Morale and Grievance Redressal Deficits**
  Issues of delayed promotions, inadequate welfare, and poor recognition erode morale, especially among lower ranks.
- **Civil–Military Tensions at the Local Level**
  Disputes over land use, seizure of smuggled goods, or enforcement during curfews can alienate local populations—who are themselves the first line of intelligence in border defence.

Conclusion

India's border guarding forces operate in some of the most inhospitable terrains on earth, from Himalayan glaciers to dense jungles and vast maritime expanses. Their effectiveness rests on courage and vigilance, but also on the urgent need for modernisation, inter-agency coordination, welfare reforms, and training for hybrid threats.

As one strategist observed:
"Our borders may be guarded by courage, but they are weakened by gaps in coordination, equipment, and empathy."

The preceding discussion shows that India's borders are protected by a diverse patchwork of forces. While this specialisation enhances resilience, it also creates overlaps, coordination delays, and fragmented accountability. A single infiltration may involve multiple agencies, but blurred authority slows decision-making.

To resolve these inefficiencies, policymakers have long advocated the principle of "One Border, One Force"—assigning clear responsibility for each frontier to a single designated agency. Though promising in theory, this model faces bureaucratic and operational hurdles in practice.

It is therefore essential to examine the origins, rationale, and challenges of the One Border, One Force policy, to understand how India can streamline command and enhance accountability in its frontier defence.

9.5 One Border, One Force Policy

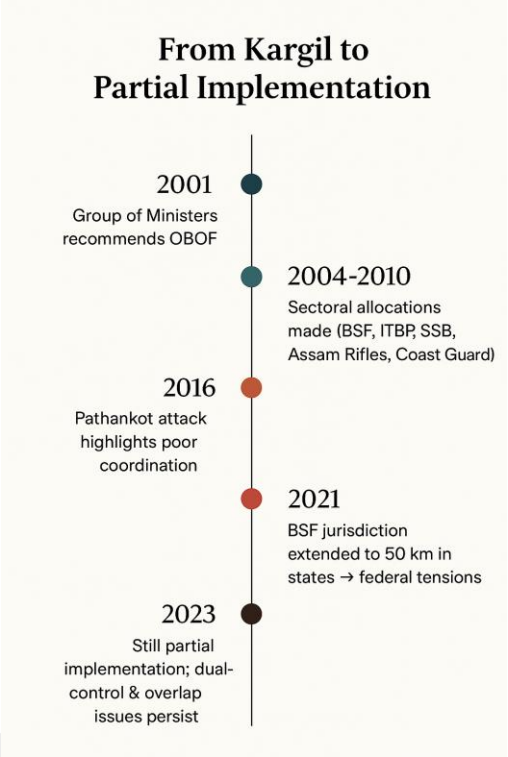
a. Background & Genesis

The principle of *One Border, One Force (OBOF)* emerged from the Group of Ministers' Report (2001), which followed the recommendations of the Kargil Review Committee. The intent was to bring clarity, efficiency, and accountability to India's sprawling border security system.

The idea was simple yet transformative: assign one specialised force to each border so that responsibility is unambiguous, training is tailored to terrain, and operational efficiency is maximised.

India's borders present extraordinary diversity—from the icy Himalayan passes of Ladakh, to the deserts of Rajasthan, the riverine belts of Assam, the jungles of the Northeast, and the 7,500-km coastline. Historically, these frontiers were patrolled by multiple agencies with overlapping jurisdictions, leading to duplication, coordination lapses, and blurred accountability.

OBOF sought to replace this patchwork with a single-point responsibility model, where one designated force would serve as the lead agency for each frontier sector. As one analyst put it:
"A single-point responsibility model ensures clearer command, focused training, and seamless deployment."



b. Objectives of OBOF

The policy was designed to achieve the following goals:

- Eliminate overlapping mandates of multiple forces in the same area.
- Enable border-specific training tailored to local terrain, culture, and threats.
- Ensure clarity of command during peace, crisis, or conflict.
- Strengthen intelligence gathering and early detection of infiltration or smuggling.
- Streamline logistics, budgets, and technology deployment under one unified chain of command.

c. Deployment Structure under OBOF

- **Western Border (Pakistan):** Border Security Force (BSF).
- **Eastern Border (Bangladesh):** BSF, including riverine stretches.
- **Northern Border (China):** Indo–Tibetan Border Police (ITBP).
- **Nepal and Bhutan Borders:** Sashastra Seema Bal (SSB).
- **Myanmar Border:** Assam Rifles (administratively under MHA, operationally under MoD).
- **Coastal Borders:** Indian Coast Guard (under MoD).

d. Gaps in Implementation

Despite its conceptual clarity, OBOF has struggled in practice:

- **Dual Control of Assam Rifles:** Its administrative control rests with the MHA, but operational command lies with the Army (MoD). This duality creates ambiguity during counterinsurgency or cross-border operations.
- **Jurisdictional Conflicts:** In 2021, BSF's jurisdiction was extended to 50 km inside Punjab, West Bengal, and Assam, leading to friction with state governments and blurred roles vis-à-vis state police.
- **Functional Overlaps:** Even today, BSF, Army, Customs, IB, and state police often operate simultaneously in border areas, leading to duplication of effort and blame-shifting.
- **Fragmented Technology & Intelligence:** Surveillance grids such as CIBMS, drone-detection systems, and AI platforms remain siloed within individual agencies, undermining real-time situational awareness.

- **Training and Doctrinal Silos:** Forces maintain separate training institutions and SOPs, with limited joint training or interoperability.
- **Bureaucratic Resistance:** Reforms recommended by the Group of Ministers have been delayed by turf battles, administrative inertia, and political sensitivities.

Illustrative Case:
The 2016 Pathankot Airbase attack exposed the costs of poor coordination. Confusion in handovers among the BSF, Punjab Police, Army, and NSG delayed response and highlighted the failure of unified command—despite OBOF being the official policy.

e. Way Forward

- **Give OBOF Legal Backing:** Convert it from a policy recommendation to a binding parliamentary mandate.
- **Resolve the Assam Rifles Duality:** Place the force under a single chain of command to avoid operational ambiguity.
- **National Border Management Grid:** Integrate surveillance, intelligence, and communication technologies across all border forces.
- **Joint Training and SOPs:** Institutionalise inter-agency training programmes and exercises for CAPFs, Army, and state police.
- **Real-Time Intelligence Sharing:** Strengthen platforms linked to NATGRID and the Intelligence Bureau to ensure rapid dissemination.

Conclusion

Two decades after its conception, OBOF remains only partially realised. While broad allocations exist—BSF for Pakistan and Bangladesh, ITBP for China, SSB for Nepal and Bhutan, Assam Rifles for Myanmar, and Coast Guard for maritime borders—serious gaps in dual control, overlapping jurisdictions, and fragmented technology persist.

As one strategist remarked:
"Borders are too strategic to be governed by silos. Security must march in a single file."

According to the MHA (2023), over 60% of border breaches involved coordination failures, underscoring the urgent need for genuine OBOF implementation.

The OBOF debate highlights that structural clarity and unified command are vital for effective border management. Yet, technology and rationalised deployments cannot substitute for the human element. Borders are not just patrolled spaces; they are lived communities.

The trust, cooperation, and vigilance of border populations—who are the first eyes and ears of the state—are indispensable to security. Harnessing community-based intelligence and local participation has thus become a critical pillar of modern border management.

It is to this human dimension—the role of border populations in safeguarding India's frontiers—that we now turn.

9.6 Community-Based Intelligence in Border Villages

a. Why Community Involvement Matters

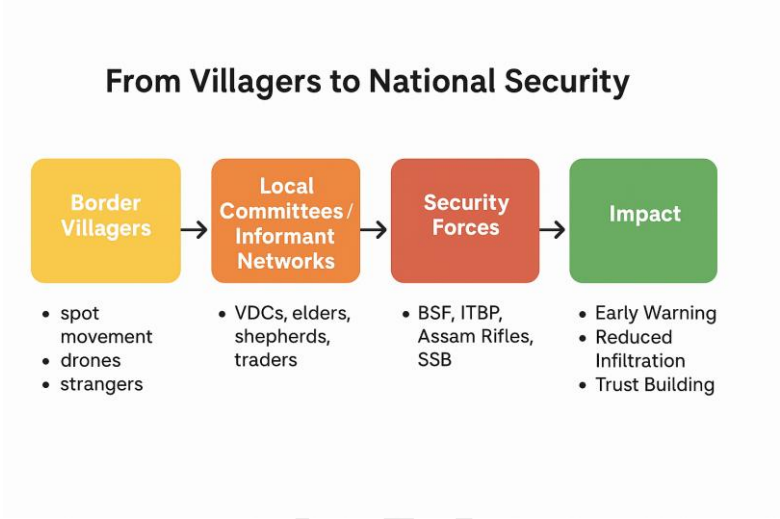
Border security in India is not defined solely by armed patrols, fences, or electronic surveillance. It is equally shaped by the vigilance, trust, and cooperation of those who inhabit frontier regions. In Ladakh's barren heights, Assam's riverine belts, the dense forests of the Northeast, and the scattered hamlets of Jammu and Kashmir, villagers are often the earliest detectors of intrusion.

Their proximity to the frontier, intimate knowledge of terrain, and deep understanding of local social patterns make them indispensable partners in early warning and rapid response. Moreover, their

active participation enhances the legitimacy of state presence in sensitive areas. As one senior BSF officer observed:
"When the State empowers villagers, borders become alert lines—not fault lines."

b. Existing Mechanisms

Over the years, India has experimented with a range of institutional and informal systems to involve border residents in security:



- **Village Defence Committees (J&K):** Formed during the militancy of the 1990s, these trained and armed villagers to defend hamlets. Recently revived in Rajouri and Poonch, they continue to serve as community militias.
- **Civic Action Programmes (CAPs):** Run by the BSF, ITBP, and Assam Rifles, these initiatives—ranging from medical camps to sports tournaments—foster goodwill and generate "soft intelligence" by deepening state–community trust.
- **Border Area Development Programme (BADP):** By building roads, schools, telecom, and water systems, BADP ties development with security, incentivising villagers to collaborate with agencies.
- **Local Informant Networks:** Shepherds, traders, village elders, and respected community figures are informally recruited to supply real-time information. Incentives and rewards strengthen their engagement.
- **Free Movement Regime (FMR):** Along the Indo–Myanmar border, tribes are allowed up to 16 km of cross-border movement. When managed effectively, this cultural continuity also doubles as a structured intelligence channel.

c. Persistent Challenges

Despite these initiatives, structural hurdles limit effectiveness:

- **Mistrust and Alienation:** In areas like the Northeast and Kashmir, historical grievances and perceived rights violations hinder cooperation.
- **Cross-Border Kinship:** Shared ethnic and tribal ties across Nepal, Bhutan, and Myanmar blur loyalties, making villagers hesitant to report kin-based intrusions.
- **Fear of Retaliation:** Informants are often targeted by terrorists, smugglers, or rival clans, with villages lacking protective infrastructure.
- **Youth Radicalisation:** Disaffected youth face narcotics abuse, extremist propaganda, and gang recruitment, eroding community resilience.
- **Weak Institutional Integration:** Much of community intelligence remains ad hoc, poorly verified, and without structured reporting systems, reducing its reliability and utility.

d. Way Forward

To transform communities into reliable intelligence partners, several steps are critical:

- **Institutionalise Vigil Groups:** Place them under CAPFs like the BSF or SSB, supported by stipends, legal backing, and basic security training.
- **Secure Tech-Enabled Platforms:** Create anonymous tip lines, encrypted mobile apps, and AI-enabled bots for real-time, safe reporting.
- **Provide Surveillance Tools:** Equip villages with watchtowers, night-vision cameras, and even drones for grassroots monitoring.
- **Link Development with Security:** Tie BADP incentives to measurable contributions—reward villages that help reduce smuggling, infiltration, or arms flows.
- **Protect Whistleblowers:** Extend witness protection schemes and security cover to at-risk informants to counter fear of retaliation.

Conclusion

Community-based intelligence transforms India's 5,000+ border villages into early-warning outposts. By bridging the gap between distant patrols and ground realities, empowered villagers shift from passive bystanders to active partners in national security.

As a 2023 Ministry of Home Affairs field report concluded:
"A border without its people is just a fence; with its people, it becomes a wall of trust."

Effective frontier management thus depends not only on boots, bunkers, or technology, but equally on legitimacy, trust, and cooperation with border populations.

Yet, while community intelligence strengthens the internal fabric of border management, India's challenges are also shaped by the external dimension of border disputes—ranging from the ambiguous Line of Actual Control with China, to unsettled riverine boundaries with Bangladesh, to recurring issues of grazing rights, fishing zones, and cross-border enclaves with Nepal and Myanmar.

This underscores that border management is as much about diplomacy and interstate negotiation as it is about surveillance and patrol. The next section therefore turns to the bilateral and multilateral mechanisms through which India and its neighbours attempt to manage contested borders, prevent escalation, and institutionalise cooperation.

9.7 Border Dispute Management Mechanisms – India and Neighbours

a. Introduction

India's borders are not mere geographical demarcations; they are deeply political, economic, and cultural frontiers. Many of them continue to bear the imprint of colonial legacies, contested maps, and unsettled sovereignty claims. Some, such as the Line of Actual Control (LAC) with China, remain undefined and contested, while others—such as those with Nepal and Bangladesh—require constant engagement to prevent historical grievances from resurfacing.

Border disputes are rarely about land alone.
They shape national security, trade flows, people-to-people ties, and regional stability. Even minor disagreements, if mismanaged, can spiral into military standoffs or prolonged mistrust. The Galwan clash of 2020 illustrated how ambiguities along the LAC can ignite sudden violence, while recurring tensions over Kalapani and Lipulekh with Nepal reveal how cartographic disputes can quickly escalate into political crises.

Managing such disputes requires a multi-pronged approach: sustained diplomacy, technical precision in surveying and mapping, and confidence-building measures (CBMs) at both the military and

community levels. As one Indian diplomat noted:
"Borders are not just about territory—they are about trust. Where dialogue builds, danger retreats."

b. Dispute Resolution Mechanisms – Country Wise

- **China (Line of Actual Control)**
  The India–China boundary lacks a mutually accepted map, making perception-driven patrol clashes inevitable. Mechanisms include:
  - **Border Personnel Meetings (BPMs):** Held at designated points such as Chushul, Nathu La, and Bum La.
  - **Working Mechanism for Consultation and Coordination (WMCC):** Diplomatic-level mechanism for crisis management.
  - **Special Representatives Dialogue:** Led by India's NSA and the Chinese counterpart, tasked with exploring boundary settlement.
- **Pakistan (Line of Control and International Border)**
  Mechanisms include:
  - **DGMO Hotline:** A vital channel for clarifying incidents and preventing escalation.
  - **Flag Meetings:** Conducted at sector levels to resolve localised tensions.
  - **UNMOGIP:** Present since 1949, though India considers it irrelevant post-1972 Simla Agreement.
- **Bangladesh**
  A landmark achievement was the 2015 Land Boundary Agreement (LBA), which resolved 161 enclaves and settled demarcation gaps, affecting over 51,000 residents.
  - Joint Border Working Groups and annual BSF–BGB meetings provide continuity in cooperation, tackling migration, smuggling, and local disputes.
- **Nepal**
  Despite friendly ties, disputes persist in Kalapani, Lipulekh, and Susta.
  - Managed through the Joint Technical Committee and diplomatic channels, though cartographic interpretations and local politics continue to fuel friction.
- **Bhutan and Myanmar**
  While Bhutan's border with India is relatively peaceful, security coordination is managed by the SSB.
  - With Myanmar, Border Liaison Meetings between Assam Rifles and local Myanmar commanders, supplemented by tribal consultations, help contain insurgency-linked tensions.

c. Shortcomings and Gaps

Despite institutional mechanisms, effectiveness is limited by:

- **Undemarcated LAC:** With no agreed map, India and China's differing perceptions result in frequent standoffs in Galwan, Tawang, and Yangtse.
- **Reactive Diplomacy:** Engagement often occurs after escalations, rather than through proactive, sustained dialogue.
- **Weak Legal Frameworks:** Lack of enforceable protocols for joint patrolling or verification leaves grey zones vulnerable.
- **Limited CBMs:** Symbolic exercises exist but remain inadequate in high-friction sectors.
- **Sub-National Pressures:** Local politics—such as ethnic grievances in the Northeast, Sikh mobilisation in Punjab, or Gorkhaland agitation in Bengal—often complicate central negotiations.

d. Way Forward

To move from crisis management to durable stability, India should:

- Institutionalise Permanent Boundary Commissions with legal authority for surveying, arbitration, and structured dispute resolution.
- **Digitise and Finalise Maps:** Deploy GIS and satellite imagery to establish jointly verified maps, particularly with China and Nepal.
- **Deepen Civil–Military Diplomacy:** Expand people-to-people CBMs such as border trade fairs, youth exchanges, and cultural initiatives.
- **Encourage Track II Diplomacy:** Academic and civil-society dialogues can supplement official negotiations.
- **Economic Linkages:** Tie border peace with tangible benefits such as cross-border trade, infrastructure, and energy projects.

SUCCESS STORY

INDIA–BANGLADESH LAND BOUNDARY AGREEMENT, 2015

- Resolved 68-year dispute
- Exchanged 161 enclaves
- Impact: 51,000+ residents integrated with chosen nationality

Lesson: Sustained diplomacy + legal treaty = durable peace

Conclusion

Effective dispute management is a strategic necessity for India, given that over 7,000 km of frontiers remain contested or politically sensitive. Sustained dialogue, verified mapping, and robust CBMs can transform disputed borders from fault lines into corridors of cooperation.

The 2015 India–Bangladesh Land Boundary Agreement stands as a landmark precedent—proving that even disputes lingering for decades can be resolved peacefully when political will is matched with structured diplomacy.

As a 2023 MEA policy brief observed:
"Borders are secured not just by force, but by the frequency and sincerity of dialogue."

The discussion so far has shown that India's borders—whether on land, river, or sea—are not just geographical spaces, but arenas where diplomacy, infrastructure, technology, and community participation converge. Yet, no amount of fencing, mapping, or dispute resolution is effective without the institutions and personnel tasked with executing them.

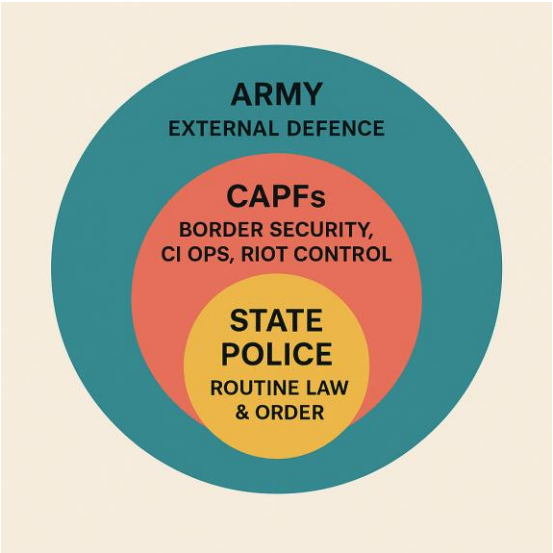
India's security grid is held together by a diverse set of forces and agencies—from the BSF on the LoC to the ITBP in the icy Himalayas, from the Coast Guard on the seas to intelligence agencies countering narco-terror, cyber threats, and insurgency. Each carries a unique mandate, but together they form the interlocking shield of national security.

Having explored the physical and diplomatic aspects of border management, we now turn to the institutional dimension—the Security Forces and Agencies of India, their structures, coordination challenges, and evolving role in hybrid warfare.

Chapter 10. Security Forces and Agencies

10.1 Central Armed Police Forces (CAPFs): Role, Structure & Challenges

a. Introduction



The Central Armed Police Forces (CAPFs) form the backbone of India's internal security and border management framework. Functioning under the Ministry of Home Affairs (MHA), they occupy the critical middle ground between the civil police, whose mandate is routine law enforcement, and the military, whose primary responsibility is external defence.

Deployed across some of the most diverse and demanding operational theatres in the world, the CAPFs shoulder a spectrum of responsibilities. The Indo–Tibetan Border Police (ITBP) monitors the icy Line of Actual Control in Ladakh; the Border Security Force (BSF) patrols the riverine belts of Assam and the desert frontiers of Rajasthan; the Central Reserve Police Force (CRPF) leads counter-insurgency operations in the Maoist-affected heartlands; and the National Security Guard (NSG) remains India's elite counter-terror strike unit for urban crises. Together, these forces constitute an integrated security shield that sustains India's sovereignty and internal order.

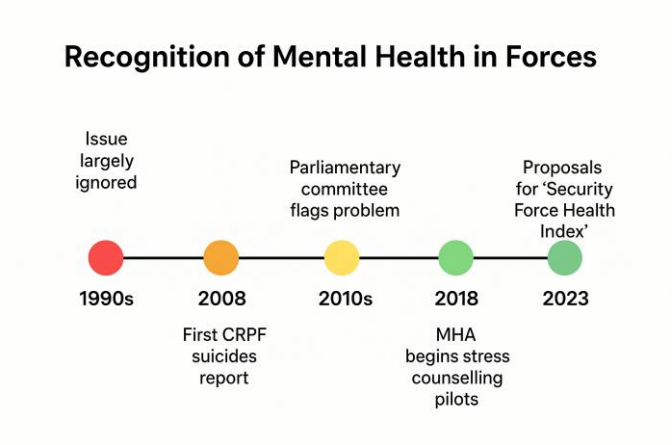
What makes their role especially demanding is the dual burden they carry. On the one hand, they are expected to perform military-style operations without the logistical depth or institutional privileges of the Army. On the other, they undertake policing-style duties without the community proximity or grassroots intelligence that state police enjoy. This duality makes them the unsung *internal frontliners* of the nation. As one senior security official put it:
"Where the Army ends and the Police fall short—CAPFs step in."

b. List of CAPFs and Their Specialised Roles

- **Central Reserve Police Force (CRPF):** India's largest paramilitary force, tasked with riot control, crowd management, combating Left-Wing Extremism (LWE), and assisting state police during elections and emergencies. It remains heavily deployed in Jammu and Kashmir.
- **Border Security Force (BSF):** Guards the Indo–Pakistan and Indo–Bangladesh borders, conducts counter-infiltration and anti-narcotics operations, and acts as the first responder to ceasefire violations.
- **Indo–Tibetan Border Police (ITBP):** Secures the Line of Actual Control with China across Ladakh, Himachal Pradesh, Uttarakhand, and Arunachal Pradesh, specialising in high-altitude survival, mountain warfare, and Himalayan disaster relief.
- **Sashastra Seema Bal (SSB):** Deployed along the open borders with Nepal and Bhutan, counters smuggling, narcotics, and human trafficking, while also building grassroots intelligence networks.
- **National Security Guard (NSG):** Popularly known as the *Black Cats*, this elite strike force specialises in counter-terrorism, hostage rescue, bomb disposal, and VVIP protection.
- **Central Industrial Security Force (CISF):** Protects airports, metros, nuclear plants, refineries, ports, and critical public-sector undertakings, while also leading India's industrial disaster response architecture.

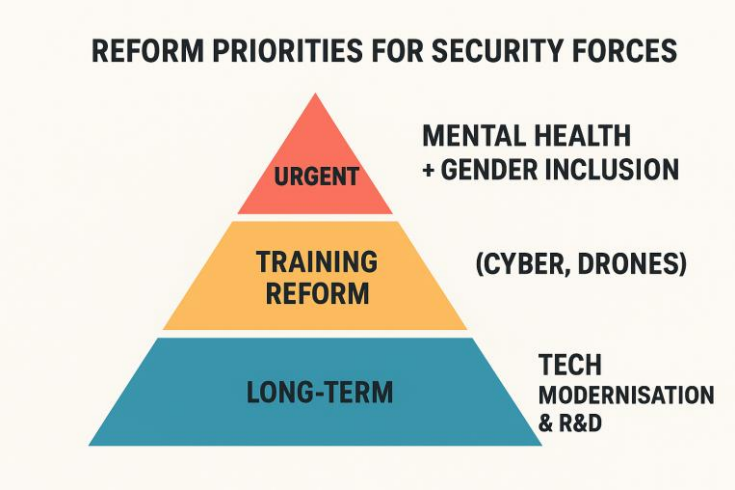
c. Challenges Faced by CAPFs

- **Overdeployment and Operational Fatigue**
    - Units, especially CRPF and BSF, are over-stretched across insurgency zones, Kashmir Valley duties, election security, VIP protection, and disaster response.
    - Some battalions remain in conflict postings for nearly a decade without relief rotations, leading to exhaustion and lowered tactical efficiency.



- **Modernisation Deficit**
    - Delays in procurement leave forces short of drones, GPS-based tracking, AI-enabled surveillance, smart riot gear, bulletproof vehicles, and mine-resistant carriers.
    - Anti-drone technologies remain scarce despite the surge in drone-based arms and narcotics infiltration along Punjab and J&K.
- **Terrain-Specific Training Gaps**
    - Forces operate across deserts, jungles, mountains, and coasts, yet training is not consistently terrain-specific.
    - Jungle warfare courses (Bastar) or high-altitude drills (Sikkim) remain limited to select units, leaving others underprepared.
- **Coordination and Role Ambiguity**
    - CAPFs often share space with the Army, state police, and intelligence agencies without a unified command.
    - The 2021 Sukma ambush—where poor coordination between CRPF and District Reserve Guards cost 22 lives—illustrates the danger of fragmented intelligence and unclear command.
- **Mental Health Crisis**
    - Continuous deployment in high-stress environments, coupled with family separation, has led to rising depression, PTSD, suicides, and fratricides.
    - Structured counselling services remain scarce.
- **Gender Underrepresentation and Bias**
    - Women constitute only about 3% of CAPFs, with higher representation in CRPF women's battalions.
    - Many units lack basic amenities for women, and underrepresentation in combat roles limits inclusivity.
- **Limited Career Progression and Grievance Redressal**
    - Constabulary ranks face stagnant promotions and lack parity with military counterparts in pensions and service benefits.
    - Grievance mechanisms are often perceived as inaccessible or biased.
- **Political and Bureaucratic Interference**
    - Deployment during elections, protests, or communal unrest is sometimes guided by political considerations.
    - Postings and transfers occasionally suffer from non-merit factors, undermining professionalism.

d. Way Forward for Strengthening CAPFs



- **National CAPF Deployment Policy:** Enforce defined rotation cycles, ensuring rest and recovery to reduce fatigue.
- **Fast-Track Modernisation:** Establish a dedicated MHA procurement wing with quarterly Cabinet reviews to speed up induction of AI, UAVs, anti-drone tech, and mobile command centres.
- **Terrain-Specific Training Academies:** Expand specialised schools for jungle warfare, high-altitude combat, and urban counter-terror, using simulations and real-case studies.
- **Unified Counter-Insurgency Commands:** Introduce theatre-style integrated commands for Maoist areas, Kashmir, and the Northeast, combining CAPFs, state police, and Army assets.
- **Mental Wellness Programmes:** Institutionalise regular psychological screening, recruit trauma counsellors, and set up confidential helplines and peer-support structures.
- **Gender Inclusion:** Mandate 10% induction of women by 2030, create women-led Quick Reaction Teams, and ensure equal facilities at postings.
- **Career and Parity Reforms:** Speed up promotions, link pay increments to hardship postings, and move towards parity in pensions and benefits with the armed forces.
- **Comprehensive CAPF Act:** Standardise powers, responsibilities, and accountability across all forces, with mandatory adoption of tech tools such as bodycams, surveillance logs, and AI-enabled monitoring.

Conclusion

With nearly one million personnel, the CAPFs are the primary shield of India's internal security, deployed across its toughest terrains and most volatile zones. Their success hinges not just on courage, but on modernisation, coordinated commands, and welfare reforms. Strengthening CAPFs is, therefore, not only a matter of security but also an investment in state resilience.

As the MHA noted in its 2023 review:
"Internal peace walks on the boots of those who guard without glory."

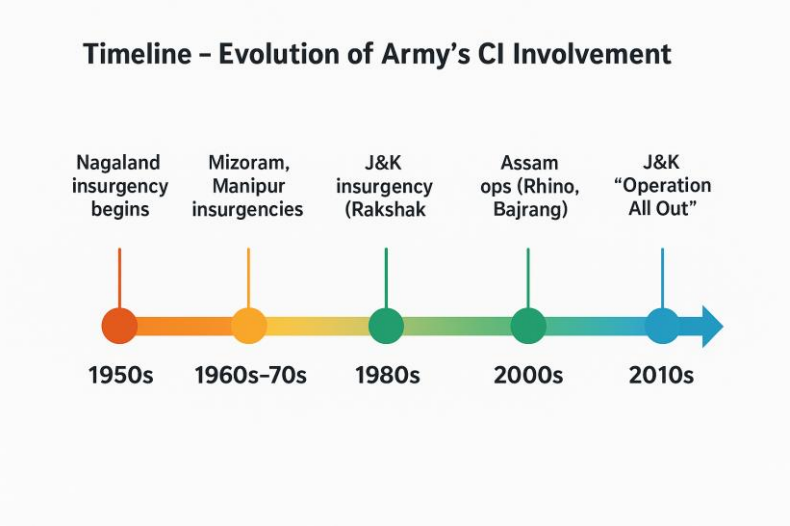
Yet, a sobering reality remains: CAPFs manage over 70% of India's counter-insurgency and border deployments, but less than 15% of their budgets are earmarked for modernisation.

The CAPFs thus represent India's internal frontliners, straddling the grey zone between soldiering and policing. But there remain theatres where their capacities are not enough—where insurgencies escalate beyond paramilitary control, or adversaries exploit cross-border sanctuaries. In such moments, it is the Indian Army that provides the decisive counter-insurgency muscle, supported by doctrines such as *"minimum force, maximum restraint"* and specialised formations like the Rashtriya Rifles.

Having understood the role and challenges of CAPFs, we now turn to examine the Indian Army's role in Counter-Insurgency Operations—its mandate, doctrines, successes, and the dilemmas it faces in balancing security imperatives with democratic accountability.

10.2 Indian Army in Counter-Insurgency (CI) Operations

a. Introduction



The Indian Army is constitutionally mandated to defend the country from external aggression. Yet, history has repeatedly drawn it into the domestic arena, whenever insurgencies or terrorism have eroded state authority beyond the capacity of police and paramilitary forces. In such moments, the Army becomes the final guarantor of national authority, stabilising regions through counter-insurgency (CI), counter-terrorism (CT), and area domination operations.

From the Kashmir Valley since 1989, to the Northeast for over six decades, and the Punjab militancy of the 1980s, the Army has shouldered extraordinary responsibilities within India's borders. Its unique approach blends kinetic force with civic outreach—a doctrine of "minimum force, maximum restraint," often paired with hearts-and-minds initiatives to rebuild state legitimacy. As one strategist observed:
"When the State's writ is erased, the Army becomes its handwriting."

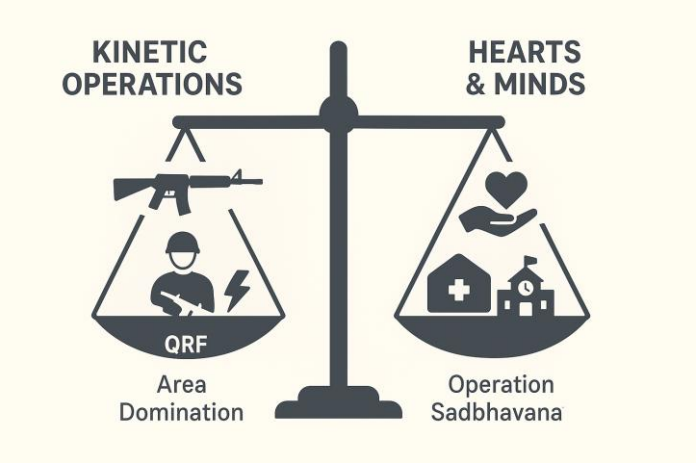
b. When and Where the Army is Deployed

- **Jammu and Kashmir**
  - The Army has been continuously deployed since the late 1980s.
  - Operation Rakshak (1990–present) remains India's longest-running counter-terror mission, integrating LoC domination with anti-infiltration sweeps and hinterland operations.
  - Rashtriya Rifles (RR), a specialised CI force raised in 1990, forms the backbone of Army operations in Kashmir.
- **Northeast India**
  - Operations against groups like ULFA, NSCN, and valley-based outfits in Manipur have been ongoing for decades.
  - These deployments rest on the Armed Forces (Special Powers) Act (AFSPA), granting extraordinary powers in "disturbed areas."
- **Punjab (Historical)**
  - The Army played a pivotal role during the 1980s militancy.
  - Operation Blue Star (1984), to flush militants from the Golden Temple, remains the most controversial.
  - Throughout the decade, Army support helped police-led campaigns crush insurgency.
- **Central India (Maoist Belt)**
  - Here, the Army has not been directly deployed but provides training, advisory support, and logistics to CAPFs.
  - Jungle warfare schools, IED handling, and operational planning are key contributions.

c. Roles Performed in CI Operations

- **Kinetic Operations**

- Includes cordon-and-search missions, ambushes, and area domination patrols to neutralise insurgent hideouts.



- **Intelligence-Based Operations**
  - Combines human intelligence (HUMINT) from locals with technical intelligence (TECHINT) such as signal intercepts, drones, and satellite feeds.
  - Joint intelligence with IB, state units, and military intelligence has improved precision in Kashmir.
- **Area Domination & Deterrence**
  - Long-term presence in vulnerable villages reinforces state authority.
  - Examples: Kupwara domination patrols in J&K, forward bases in Manipur.
- **Hearts and Minds (Civic Outreach)**
  - Operation Sadbhavana in Kashmir provides medical camps, schools, and vocational training to win trust.
  - Similar civic actions in the Northeast improve local legitimacy of state presence.
- **Training & Capacity Building**
  - Army trains CAPFs and police in CI tactics and survival.
  - Also conducts bilateral training with partners such as Afghanistan and Myanmar.
- **Quick Reaction Forces (QRFs)**
  - Provide rapid reinforcement during crises.
  - Examples: Uri (2016) and Pulwama (2019) saw Army QRFs secure perimeters and neutralise militants.

d. Major Counter-Insurgency Operations in History

Operation	Region	Objective
Operation Blue Star (1984)	Punjab	Flush out militants from Golden Temple.
Operation Rakshak (1990–present)	Jammu & Kashmir	Long-term CI/CT mission combining LoC dominance with hinterland counter-terror.
Operation Bajrang & Rhino (1990s–2000s)	Assam	Neutralise ULFA and Bodo insurgents.
Operation Hifazat	Manipur	Target PLA and KYKL insurgents in valley regions.
Operation All Out (2017–present)	Jammu & Kashmir	Joint Army–Police–CRPF offensive to eliminate top terror leadership.

e. Challenges Faced by the Army in CI

- **Civilian Collateral Risk**

- Insurgents hide in civilian areas, risking casualties during encounters.
- Such incidents fuel alienation and unrest.

- **Legal & Political Scrutiny**
  - Reliance on AFSPA attracts criticism for alleged excesses and "fake encounters."
  - Civil society and international pressure challenge legitimacy.
- **Role Creep & Morale Issues**
  - Prolonged CI duty diverts focus from conventional warfare readiness.
  - Leads to stress and morale dips among troops trained for external combat.
- **Intelligence Gaps**
  - Unlike local police, the Army lacks deep grassroots networks, often depending on delayed or partial inputs.
- **Psychological Stress**
  - Long deployments, constant ambush risks, political hostility, and media scrutiny contribute to PTSD, burnout, and fratricide cases.

f. Way Forward

- **Clear Exit Strategy** – Army deployment should remain temporary, with eventual handover to CAPFs and police.
- **Human Rights Oversight** – Embed legal advisors, Army–NHRC liaison cells, and periodic reviews to minimise collateral harm.
- **Intelligence Fusion Cells** – Establish real-time joint ops centres integrating Army, IB, state police, and CAPFs.
- **AFSPA Reforms** – Introduce time-bound reviews and accountability mechanisms to balance immunity with oversight.
- **Counter-Radicalisation Partnerships** – Work with NGOs, teachers, and counsellors to reduce extremist recruitment.
- **Rotation & Decompression** – Institutionalise leave cycles, counselling access, and decompression postings after high-intensity CI duty.

Conclusion

The Indian Army remains the backbone of India's counter-insurgency grid, operating across over forty districts in J&K and the Northeast. Its strength lies in combining kinetic dominance with civic legitimacy, creating conditions for the return of normal governance. Yet, long-term stability demands that the Army's role remain intelligence-driven, rights-conscious, and ultimately transitional—handing back control to police and civil institutions.

As the Army doctrine (2023) affirms:
"When the State's writ is erased, the Army becomes its handwriting."

Over 65% of the Army's CI deployments are concentrated in Jammu & Kashmir alone, underscoring both the scale and persistence of India's internal security challenge.

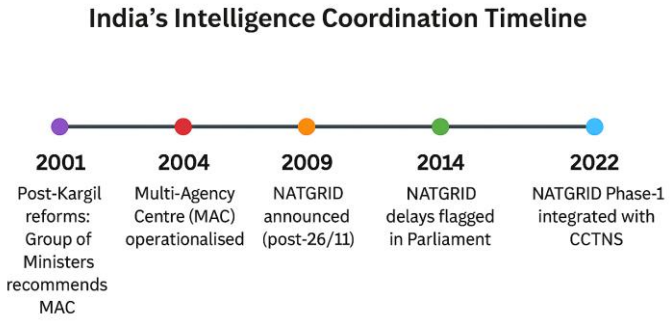
The Army's counter-insurgency success depends on timely and precise intelligence. Without actionable inputs, patrols walk into ambushes, insurgents slip across porous borders, and terror networks regenerate despite tactical victories. This invisible scaffolding of internal security is built by India's intelligence agencies—the operatives who piece together fragments from human informants, cyber grids, satellites, and financial trails.

To understand how India confronts threats that are clandestine, decentralised, and transnational, the next section turns to the intelligence apparatus—its structure, mandates, challenges, and the reforms needed to make it fit for the era of hybrid warfare.

10.3 Intelligence Agencies in India: Roles, Challenges and Reforms

a. Introduction

In the age of hybrid warfare, intelligence forms the first and most decisive line of defence. Long before counter-terror squads deploy or soldiers mobilise, it is intelligence that detects, disrupts, and deters threats—whether terrorism, cyber intrusions, narco-financing, organised crime, or foreign influence operations.



India's intelligence framework is a dual system:

- Civilian agencies such as the Intelligence Bureau (IB) and Research and Analysis Wing (R&AW) handle internal and external dimensions.
- Military intelligence agencies such as the Defence Intelligence Agency (DIA) and technical arms like the National Technical Research Organisation (NTRO) extend capabilities across conventional and cyber domains.
- Hybrid institutions like the Multi-Agency Centre (MAC) and National Investigation Agency (NIA) link intelligence with coordination and prosecution.

Yet, intelligence carries a paradox: failures are highly visible, successes invisible. As one analyst observed:
"Intelligence failures are silent disasters; successes are invisible victories."

b. Key Intelligence Agencies in India

- **Intelligence Bureau (IB)**
  - Established in 1887, it is India's oldest agency.
  - Operates under the Ministry of Home Affairs.
  - Responsible for domestic security: counter-terrorism, insurgency monitoring, surveillance, political intelligence, and VIP threat assessments.
- **Research and Analysis Wing (R&AW)**
  - Created in 1968 after the 1962 and 1965 wars.
  - Handles external intelligence, espionage, counter-espionage, strategic operations, and psychological warfare.
  - Monitors developments in Pakistan, China, and other regions critical to India's security.
- **Defence Intelligence Agency (DIA)**
  - Established in 2002 after the Kargil Review Committee's recommendations.
  - Coordinates intelligence across the Army, Navy, and Air Force.
  - Tracks adversaries' troop deployments, doctrines, and military capabilities.
- **Multi-Agency Centre (MAC)**

- Set up in 2001 after the Kargil conflict.
- Operates under the IB as a 24×7 coordination hub.
- Integrates inputs from R&AW, NTRO, NIA, military intelligence, and state police.
- Supported by State Multi-Agency Centres (SMACs) at the local level.

- **National Technical Research Organisation (NTRO)**
  - India's premier technical intelligence (TECHINT) body.
  - Specialises in signals intelligence (SIGINT), cyber espionage, encryption cracking, satellite-based surveillance, and imagery analysis.
- **National Investigation Agency (NIA)**
  - Created in 2008 after the Mumbai attacks.
  - A federal investigative agency under the NIA Act.
  - Probes terrorism, organised crime, narco-terrorism, and cyberterrorism.
  - Serves as a bridge between intelligence and prosecution.

c. Challenges in the Intelligence System

- **Absence of Legal Mandates**
  - Unlike the CIA (US) or MI6 (UK), India's IB and R&AW lack statutory status.
  - Raises accountability concerns and risks of political misuse.
- **Turf Wars and Siloed Functioning**
  - Agencies often withhold information to preserve turf.
  - Leads to duplication, mistrust, and delays during crises.
- **Coordination Gaps**
  - Despite the MAC, real-time integration is weak.
  - Inputs are sometimes lost in bureaucratic chains—seen in incidents like Pulwama (2019) and Naxal ambushes.
- **Weak Human Intelligence (HUMINT)**
  - Over-reliance on technical surveillance has weakened grassroots informant networks.
  - Lack of village-level penetration has proved costly in insurgency zones.
- **Lag in Cyber Adaptation**
  - Agencies remain underprepared for AI-powered surveillance, dark web tracking, crypto-financing, and bot-led propaganda.
- **Politicisation and Internal Surveillance**
  - Periodic accusations of using IB or state intelligence for political purposes.
  - Erodes neutrality and distracts from counter-terror and hybrid threat monitoring.

d. Way Forward – Reforming the Architecture

- **Legal Codification**
  - Enact an Indian Intelligence Services Act giving statutory clarity to IB, R&AW, and NTRO.
  - Embed accountability and safeguards against misuse.
- **Parliamentary Oversight**
  - Establish a bipartisan standing committee on intelligence.
  - Review expenditure, ethics, and performance—on the model of US/UK oversight.
- **Unified National Intelligence Grid (NATGRID)**

- Accelerate integration of banking, passports, telecom, FIRs, immigration, and tax datasets.
- Provide real-time access to vetted agencies.

- **Strengthening HUMINT**
  - Expand recruitment from local communities, linguistic minorities, and insurgency-prone belts.
  - Protect and incentivise informants through structured rewards and security cover.
- **Cyber Intelligence Corps**
  - A joint NTRO–CERT-In unit for AI-driven monitoring, deepfake detection, crypto tracking, and disinformation mapping.
- **Inter-Agency Cadre Mobility**
  - Officer rotation between IB, R&AW, DIA, NIA, and state intelligence to break silos and build an integrated culture.
- **Public–Private Partnerships**
  - Engage startups, ethical hackers, academia, and linguistic experts for OSINT, dark web monitoring, and multilingual cyber surveillance.

Conclusion

India's intelligence grid spans the domestic, external, technical, and investigative spectrum, but gaps in law, coordination, and cyber-readiness constrain its effectiveness. In a world where 80% of threats are hybrid and transnational, the future lies in seamless integration, statutory reform, and balancing secrecy with accountability.

As Sun Tzu reminded:
"Intelligence wins wars before they are fought."

MHA data (2023) reveals that 60% of major terror incidents in the past decade had prior intelligence, but failures in sharing and acting on time led to preventable casualties—a sobering reminder of systemic weakness.

The survey of agencies shows that India does not lack information—it suffers from fragmented coordination. Post-mortems of crises from Kargil (1999) to Mumbai (2008) to Pulwama (2019) point to the same structural flaw: intelligence was available but not integrated or acted upon.

Thus, the next section must examine the broader coordination architecture of national security—why silos persist, how they undermine operational effectiveness, and what reforms are required to build a truly integrated, seamless security grid for the 21st century.

Chapter 11. Police Reforms and Smart Policing

Introduction

The police form the frontline guardians of internal security, serving as the most visible link between the State and its citizens. Their mandate is vast—law enforcement, crime prevention, riot control, counter-terrorism, intelligence gathering, investigation, and community engagement. In practice, the police officer is both the first responder to crises and the day-to-day guarantor of order.

Yet, the institutional framework of policing in India continues to rest on the Indian Police Act of 1861—a colonial law designed not for democratic service, but to enforce imperial authority. While Indian society, technology, and threats have undergone seismic changes, the policing structure has remained largely unreformed.

The twenty-first century has added new layers of complexity:

- AI-driven disinformation campaigns,
- digital radicalisation,
- narco-terrorism, and
- cross-border hybrid warfare.

Such challenges demand a police system that is specialised, technology-enabled, accountable, and community-trusted. Instead, India's police struggle with political interference, vacancies, outdated training, poor infrastructure, and weak accountability mechanisms.

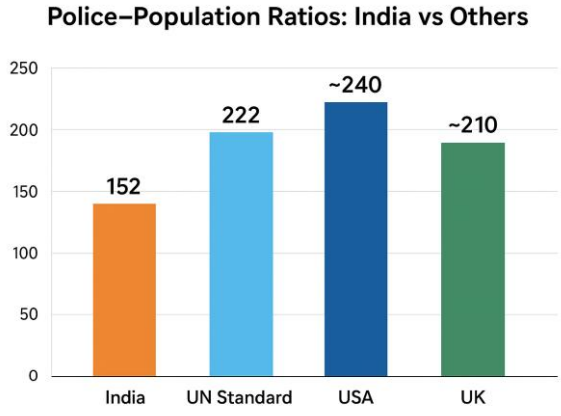
As the Second Administrative Reforms Commission (ARC) observed:
"A 21st-century democracy cannot be secured by a 19th-century police structure."

Reform, therefore, is not merely an administrative necessity—it is a national security imperative.

11.1 Challenges and Reforms Proposed in Indian Policing

a. Challenges in Indian Policing

- **Political Interference**
  - Frequent, non-merit-based transfers erode professionalism.
  - Investigations and law enforcement decisions are often influenced by political pressure, undermining neutrality and public trust.
- **Chronic Vacancies and Low Police–Population Ratio**



- India's police–population ratio is 152 per lakh, well below the UN norm of 222 per lakh.
- With over five lakh sanctioned posts vacant, the force remains severely overstretched, limiting effective patrolling, investigation, and community engagement.

- **Colonial Legacy and Role Conflict**
  - The police are still perceived as agents of rulers, not as public servants.
  - Training largely focuses on maintaining "order" rather than building community trust or citizen-centric service delivery.
- **Weak Accountability Mechanisms**
  - Independent police complaints authorities exist only on paper in most states.
  - Custodial deaths, corruption, and misconduct often go unpunished due to weak oversight and internal shielding.
- **Inadequate Infrastructure**
  - Many police stations lack:
    - vehicles,
    - secure armouries,
    - internet connectivity,
    - forensic kits, or
    - functioning cybercrime units.
  - Even designated cybercrime cells remain under-resourced despite the rise of digital offences.
- **Outdated Legal Framework and SOPs**
  - Most states continue to operate under 1861-era Police Acts, despite repeated Supreme Court directives and commissions recommending change.
  - No standardised investigation protocols exist for cryptocurrency laundering, deepfake circulation, AI-enabled fraud, or cross-border digital crime.
- **Overwork and Burnout**
  - Policemen often work 14–16 hour days, with little scope for structured rest or leave.
  - Chronic fatigue results in poor decision-making, irritability, declining professionalism, and in some cases, mental health breakdowns.

b. Reforms Proposed and Enacted

i. The Prakash Singh Case (2006)

The Supreme Court's landmark judgment on a PIL filed by former DGP Prakash Singh sought to depoliticise and professionalise Indian policing. It laid down a set of binding directives aimed at creating stability, accountability, and operational independence.

Key Directives:

- **State Security Commissions:** To insulate policy decisions from political manipulation.
- **Fixed Tenure:** A minimum of two years for DGPs, SPs, and SHOs, ensuring leadership stability.
- **Police Establishment Boards:** To make postings, promotions, and transfers transparent.
- **Separation of Functions:** Distinct wings for *law and order* versus *investigation* to improve professionalism and conviction rates.
- **Police Complaints Authorities:** At both state and district levels, to provide independent oversight of misconduct.

- **National Security Commission:** To professionalise recruitment and functioning of the CAPFs.

Status:
Implementation has been partial and diluted. Tenure security is rarely honoured, independent complaints authorities remain weak, and political influence continues to dominate postings—limiting the impact of this landmark judgment.

ii. Second Administrative Reforms Commission (2nd ARC) – 5th Report *"Public Order"* (2007)

The 2nd ARC offered one of the most comprehensive reform blueprints for policing in a democracy.

Core Recommendations:

- **Replacement of Colonial Laws:** Enact a new *Model Police Act* that reflects democratic accountability and citizen service.
- **Functional Autonomy with Accountability:** Distinguish political oversight (policy domain) from operational independence (professional domain).
- **Specialisation:** Create dedicated wings for investigation, cybercrime, economic offences, counter-terrorism, forensics, and victim support.
- **Decentralisation and Community Policing:** Empower local police through community engagement mandates and citizen advisory committees.
- **Recruitment and Training:** Merit-based recruitment with psychological testing, combined with training in human rights, gender sensitivity, and digital crime.
- **Technology Integration:** Expand IT tools, e-FIRs, predictive crime analytics, surveillance capabilities, and video conferencing systems.
- **Accountability Mechanisms:** Establish Police Complaints Authorities, enforce internal discipline, and mandate public reporting of performance.

As the report memorably stated:
"Policing should move from a force model to a service model."

iii. Modernisation of Police Forces (MPF) Scheme

Launched in 2000 and revamped in 2017, the MPF Scheme was the first mission-mode programme to upgrade state and UT police forces.

Objectives:

- Enhance mobility, communication, and weaponry.
- Improve infrastructure—barracks, housing, cyber labs, and forensic facilities.
- Integrate IT systems, including CCTNS (Crime and Criminal Tracking Network and Systems) and ICJS (Inter-Operable Criminal Justice System).
- Strengthen capacity in Left-Wing Extremism (LWE)-affected areas.

Key Components:

- **Mobility Support:** Patrol vehicles, motorcycles, boats for coastal surveillance, and drones in select states.
- **Weapons and Protective Gear:** Modern rifles, bulletproof jackets, night-vision equipment, and non-lethal riot gear.
- **Infrastructure:** Police stations, barracks, wireless towers, and housing for constables in remote regions.
- **Technology Integration:** CCTNS, ICJS, and fingerprint/biometric systems.
- **Training and Cyber Units:** Funding for cyber forensics, AI modules, and modern police academy curricula.

- **Special Provisions for LWE Areas:** Fortified police stations, intelligence cells, and advanced equipment.

Persistent Challenges:

- **Low State Utilisation:** Many states fail to use central funds effectively.
- **Lack of Standardisation:** Independent procurement creates inefficiencies and inconsistency.
- **Weak Monitoring:** Poor MIS dashboards make implementation difficult to track.
- **Urban Bias:** Resources concentrate in capital cities, neglecting rural/tribal districts.
- **Poor Lifecycle Management:** Equipment maintenance and periodic upgrades are overlooked.

Conclusion

India's 22 lakh police personnel form the bedrock of internal security, yet remain overworked, under-equipped, and constrained by colonial legacies and political interference. Police reform is not just a governance necessity but a national security imperative.

The path forward requires:

- Insulating the police from partisan politics,
- Embedding technology and digital tools,
- Professionalising recruitment and training,
- Establishing genuine accountability mechanisms, and
- Fostering a culture of citizen-centric service.

As the 2nd ARC reminded us:
"Policing in a democracy must protect both security and liberty—or it protects neither."

India's police–population ratio stands at 152 per lakh, against the UN norm of 222 per lakh, leaving over five lakh posts vacant—a gap that weakens the State's first line of defence.

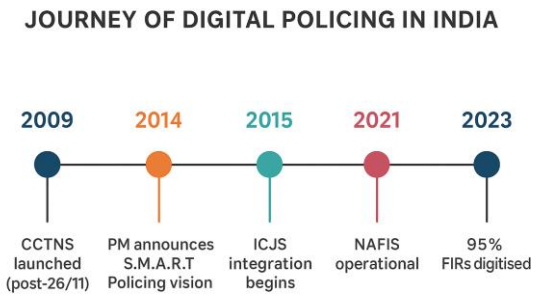
The preceding discussion has shown how structural reforms, legal mandates, and modernisation schemes are essential for transforming India's police into a professional and citizen-oriented force. Yet, even the best-designed legislation cannot by itself prepare the police for 21st-century threats like cybercrime, AI-driven disinformation, or drone-enabled smuggling.

This is where Smart Policing becomes pivotal—a shift from manpower-heavy, reactive law enforcement to technology-enabled, predictive, and citizen-trusted policing. Having surveyed the reform blueprint, we now turn to Smart Policing Initiatives that are already reshaping Indian policing—from e-FIRs and predictive analytics to AI-driven surveillance, cyber labs, and citizen-service apps.

11.2 Smart Policing Initiatives

a. Introduction

In the age of data-driven governance and hybrid threats, policing can no longer remain manpower-intensive or reactive. The future lies in intelligence-led, technology-enabled, and citizen-centric policing that anticipates crime rather than merely responds to it. This vision was formally articulated in 2014 through the concept of S.M.A.R.T Policing—Strict and Sensitive, Modern and Mobile, Alert and Accountable, Reliable and Responsive, Tech-savvy and Trained.



Smart policing is not confined to surveillance or gadgets; it represents a shift in policing philosophy. It emphasises speed, transparency, and trust—using digital platforms, predictive analytics, biometrics, integrated command systems, and citizen-facing mobile applications to make law enforcement both more effective and more democratic.

India's transition is already visible in national platforms like CCTNS and ICJS, and state-led innovations such as Telangana's Hawk Eye or Kerala's Janamaithri. Together, they mark the move from reactive enforcement to proactive prevention, securing society while safeguarding liberty.

i. Key Digital and Data-Driven Platforms

- **Crime and Criminal Tracking Network and Systems (CCTNS):** Digitises FIRs, arrest records, and case files, connecting over 95% of police stations nationwide and enabling real-time tracking of cases.
- **Inter-Operable Criminal Justice System (ICJS):** Links police databases with courts, forensic labs, prisons, and prosecution wings, reducing trial delays.
- **National Automated Fingerprint Identification System (NAFIS):** A centralised fingerprint repository of over ten crore records for rapid identification across states.
- **e-FIR and Online Complaint Portals:** Allow citizens to lodge FIRs for non-cognisable offences remotely, crucial for rural and remote regions.
- **AI-Powered Predictive Policing:** Piloted in Hyderabad, Delhi, and Bhopal, algorithms analyse crime patterns to predict hotspots and optimise patrols.
- **Facial Recognition Systems (FRS):** Deployed in railway stations and crowded areas to trace missing persons and detect suspects in real time.

ii. Helplines, Mobile Apps, and Community Tools

- **112 India App:** A nationwide emergency response platform integrating police, ambulance, fire, and women's helplines, with a panic button feature.
- **Prahari App (Assam Rifles):** Facilitates field reporting, real-time tracking, and soldier welfare monitoring in border regions.
- **National Cybercrime Reporting Portal:** Provides a central platform to report online fraud, child exploitation, and financial crime.
- **Beat App Integration:** Tracks constables through GPS, digitises e-verification, and improves accountability at the local level.
- **Himmat App (Delhi Police):** A women's safety tool enabling SOS alerts and live GPS tracking directly linked to police control rooms.

iii. State-Level Innovative Projects

State	Initiative	Description
Telangana	Hawk Eye App	Citizen app for women's safety, crime reporting, traffic complaints, and lost item recovery.
Kerala	Janamaithri Policing	Focuses on house visits, community patrols, and youth club engagement to build trust.
Tamil Nadu	Friends of Police	A civil-society partnership encouraging citizen volunteers in local policing tasks.
Madhya Pradesh	Black Panther Force	Special tribal counter-insurgency units designed for operations in Left-Wing Extremism areas.

Conclusion

Smart policing is gradually transforming Indian law enforcement into a digitally connected, tech-empowered, and citizen-responsive service. With more than 16,000 police stations digitised under CCTNS and predictive policing already active in several cities, the foundations of modern policing are firmly in place. The next challenge lies in scaling innovations across all states, bridging rural–urban divides, and ensuring that technology strengthens both security and liberty.

As one reformer put it:
"The police station of the future will be as much a data hub as a duty post."

According to the Ministry of Home Affairs (2023), CCTNS has digitised over 95% of FIRs nationwide, enabling seamless case-tracking across more than 16,000 police stations.

While smart policing showcases how technology enhances efficiency and transparency, machines and algorithms alone cannot secure a democracy. The essence of policing lies in trust, built not by cameras or AI dashboards, but through relationships with citizens.

Experiments like Kerala's *Janamaithri* and Tamil Nadu's *Friends of Police* demonstrate that when citizens become partners rather than passive subjects, policing becomes preventive, inclusive, and humane.

Having examined the technological dimension of reform, we now turn to the human dimension: Community Policing Models in India—their evolution, practices, and potential to transform the police from an instrument of authority into an institution of partnership.

11.3 Community Policing Models in India

a. Introduction

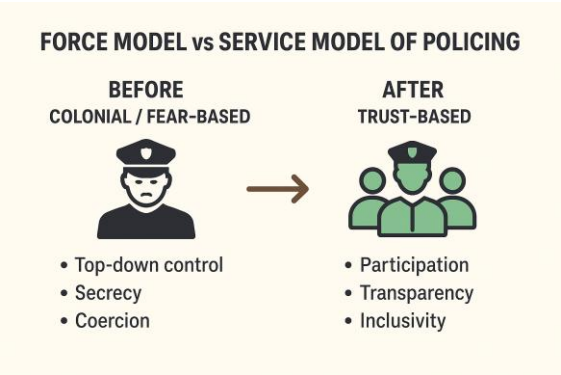
Community policing represents a shift in philosophy: from policing as a force of control to policing as a facilitator of civic harmony and social order. At its core, it is a partnership model, where the police and the public collaborate to build trust, prevent crime, and solve local problems collectively. Its strength lies in mutual respect, regular engagement, and shared responsibility for security.

In a country as diverse as India—marked by region-specific security challenges, deep cultural variations, and historical mistrust of authority in certain areas—community policing serves as a powerful force multiplier. By leveraging the vigilance, knowledge, and networks of local citizens, it transforms communities from passive recipients of policing into active partners of security. Women-led night patrols in Manipur, youth clubs in Kerala, or beat officer systems in states nationwide show how local participation enhances resilience against crime, conflict, and radicalisation.

As one reformer aptly put it: *"Policing is effective not because of fear—but because of faith."*

b. Core Objectives of Community Policing

- Build enduring trust between citizens and police.
- Encourage public participation in crime prevention and intelligence sharing.
- Develop localised solutions tailored to community-specific problems.
- Address root causes of conflict such as drug abuse, domestic violence, or youth delinquency.



- Establish early-warning systems in areas prone to communal tension or radicalisation.

c. Prominent Community Policing Models in India

Model	State/Region	Key Features	Impact
Janamaithri Suraksha Project	Kerala	Beat officers conduct house visits, neighbourhood groups, local problem-solving meetings, and youth club engagement.	Won SKOCH Award; built strong police–public trust, esp. in minority areas.
Meira Paibi (Torch Bearers)	Manipur	Women-led night patrols, drug abuse prevention, family mediation, cooperation in CI operations.	Reduced drug abuse, lowered insurgent influence, curbed domestic violence.
Mitra Yojana	Maharashtra	Engages auto drivers, shopkeepers, and students as "eyes and ears" of the police.	Strengthened grassroots intelligence; effective during festivals and rallies.
Friends of Police (FoP)	Tamil Nadu	Civilian volunteers assist in traffic control, women's safety, disaster response; feedback channels included.	Replicated widely; cost-effective multiplier of police presence.
Beat System	Pan-India	Division of station areas into beats; officers handle surveillance, outreach, intelligence gathering.	Improved crime mapping, quick redressal, and trust in policing.

d. Key Pillars of Successful Community Policing

- **Trust Building:** Sustained outreach, grievance redressal, and police visibility beyond crises.
- **Volunteerism:** Harnessing the role of youth, women, ex-servicemen, and civil society groups.
- **Inclusivity:** Targeting vulnerable groups—tribals, minorities, women, elderly—for deeper participation.
- **Transparency:** Public dashboards, community meetings, and open access to complaint updates.
- **Technology Integration:** Mobile apps, helplines, and WhatsApp groups for real-time interaction.
- **Problem-Solving Orientation:** Addressing structural causes like poor lighting, recurring disputes, or unsafe transport, rather than focusing solely on incident response.

e. Challenges in Implementation

- **Low Officer Motivation:** Many personnel view outreach as secondary, with limited training or incentives.
- **Volunteer Fatigue:** Community members disengage without recognition or follow-up support.
- **Urban–Rural Divide:** Urban pilots thrive with resources, while rural models face thin manpower and diverse populations.
- **Cultural Barriers:** Historical mistrust in Kashmir or parts of the Northeast limits participation.
- **Funding Gaps:** Most projects depend on pilots or ad hoc grants, lacking continuity.
- **Weak Monitoring:** No standardised evaluation frameworks to assess impact or scale successful models.

f. Way Forward

- Establish Community Policing Cells at district level with dedicated resources and officers.
- Incentivise Volunteers through recognition, training, and honorary status to sustain long-term engagement.
- Launch Youth Engagement Hubs in schools and colleges to prevent radicalisation and nurture early trust.
- Leverage Technology via mobile apps, WhatsApp groups, and local dashboards for faster interaction.
- Conduct Quarterly Social Audits to evaluate performance and adapt strategies.
- Provide Specialised Training in mediation, cultural sensitivity, and surveillance basics for both officers and volunteers.

Conclusion

Community policing redefines the relationship between state and society, transforming citizens into co-producers of security. With over 1.5 lakh beat officers engaged in outreach nationwide, scaling up such models can multiply effectiveness without expanding manpower proportionally. The real objective is not only safer neighbourhoods, but stronger bonds of trust between citizens and the law.

As one field report concluded: *"A citizen who trusts the police becomes the first responder of the law."*

Kerala's *Janamaithri Suraksha Project* has recorded over 90% citizen satisfaction in independent surveys, proving the tangible success of trust-led policing.

The preceding chapter demonstrated how reforms, technology, and community partnerships can transform policing. Yet, even the most citizen-friendly police model must operate within the framework of law and democracy. Internal security is not simply about capacity—it is equally about legitimacy.

India's security landscape is fraught with legal and ethical dilemmas: the use of extraordinary laws such as AFSPA and UAPA, the tension between surveillance and privacy, the balance between counter-terror powers and human rights, and the challenge of accountability while enabling swift state action.

Having analysed the operational pillars of internal security, we now turn to its normative foundations: the legal and ethical issues that shape how India protects itself without compromising its constitutional ethos.

Chapter 12. Legal & Ethical Issues in Internal Security

Introduction

Internal security in a democracy operates at the intersection of national safety and constitutional morality. While the State must be empowered to deal with insurgency, terrorism, and hybrid threats, it must also uphold fundamental rights, due process, and public trust.

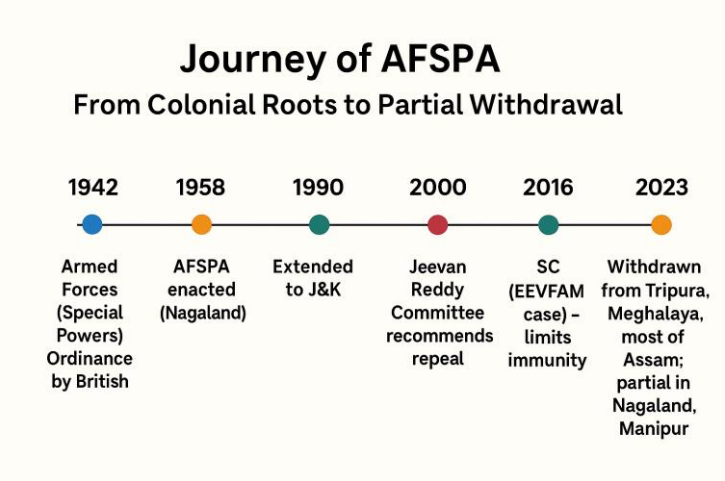
Legal provisions like the Armed Forces (Special Powers) Act (AFSPA), the Unlawful Activities (Prevention) Act (UAPA), and various surveillance laws give security agencies extraordinary powers. Yet, these very provisions raise ethical questions about accountability, proportionality, and human rights. This chapter examines such powers, the criticisms they attract, and the reforms required to balance security with justice.

"National security must be the shield of democracy, not its blindfold."

12.1 The Armed Forces (Special Powers) Act (AFSPA)

a. Introduction

The Armed Forces (Special Powers) Act, 1958, is among the most controversial components of India's internal security framework. Conceived in response to rising insurgencies in the Northeast, it was modelled on the Armed Forces Special Powers Ordinance of 1942—a colonial instrument used by the British to suppress the Quit India Movement.



AFSPA empowers the armed forces to operate in areas declared "disturbed," providing them with extraordinary authority approximating martial law, though without formally declaring it.

The rationale was straightforward: in regions where civilian administration was unable to maintain order, the Army required legal backing to act swiftly and decisively against insurgents. Over time, the Act was extended beyond the Northeast to Jammu and Kashmir and other border states.

As one scholar noted, *"AFSPA was meant as a shield for the soldier, but it became a symbol of fear for the citizen."*

b. Objectives of AFSPA

The Act was designed to enable the armed forces to:

- Operate in disturbed areas where law and order has collapsed.
- Counter armed insurgency, terrorism, or organised rebellion.
- Act without bureaucratic delay in situations demanding rapid force.

Since its enactment, AFSPA has been applied in Nagaland (since 1958), Jammu and Kashmir (1990–2020), and parts of Manipur, Assam, and Arunachal Pradesh.

c. Key Provisions of the Act

Section	Power Granted
Section 3	Authorises Governor or Centre to declare any area "disturbed."
Section 4(a)	Permits armed forces to use force, even to the extent of causing death, on suspicion.
Section 4(b)	Authorises destruction of arms dumps, fortified positions, or insurgent hideouts.
Section 4(c)	Allows arrest without warrant of any person suspected of committing or about to commit a cognisable offence.
Section 4(d)	Permits search and seizure without warrant.
Section 6	Grants immunity from prosecution: no legal proceeding can be initiated without prior sanction of the Central Government.

In practice, these provisions grant sweeping powers to the Army, often indistinguishable from emergency or martial law conditions.

d. Criticisms and Human Rights Concerns

- **Violation of Rights**: Incidents such as the Malom Massacre (2000) in Manipur, where ten civilians were killed, and the custodial killing of Manorama Devi (2004), have become rallying points against AFSPA.
- **Impunity**: Despite repeated allegations of torture, rape, and fake encounters, prosecutions remain rare due to Section 6 immunity.
- **Alienation**: Prolonged military presence under AFSPA has often deepened resentment, particularly among youth, fuelling cycles of insurgent recruitment.
- **Legal Black Hole**: Immunity provisions effectively block even the registration of FIRs, creating what critics call a "zone of exception."
- **Global Scrutiny**: The United Nations Human Rights Council and Amnesty International have described AFSPA as incompatible with international conventions such as the International Covenant on Civil and Political Rights (ICCPR).

As the National Human Rights Commission observed in 2013, *"The presence of the Army should assure safety, not instil fear."*

e. Jeevan Reddy Committee Report (2005)

Commissioned by the Government of India, the Justice B. P. Jeevan Reddy Committee made bold recommendations on AFSPA:

- **Repeal AFSPA**: Concluded that the Act had become a symbol of oppression and a liability.
- **Integrate Provisions into UAPA**: Suggested retaining necessary operational powers under the Unlawful Activities (Prevention) Act without blanket immunity.
- **Civilian Oversight**: Recommended creation of independent grievance redressal mechanisms.
- **Periodic Review**: Proposed making the "disturbed area" status subject to six-monthly reviews.

- **Strengthen Civil Institutions**: Urged capacity-building of local administration and police to reduce reliance on the Army.

Despite its significance, the report was never implemented, leaving AFSPA largely intact.

f. Supreme Court's Intervention (2016)

In *EEVFAM vs Union of India*, the Supreme Court redefined the scope of AFSPA and sought to introduce accountability:

- **No Absolute Immunity**: Held that Army actions leading to civilian deaths must be subject to investigation.
- **Rule of Law Applies**: Asserted that even in disturbed areas, fundamental rights cannot be suspended indefinitely.
- **Probe into Fake Encounters**: Ordered investigation into 1,528 alleged extrajudicial killings in Manipur.
- **Proportionality Doctrine**: Clarified that the use of force must be minimum, necessary, and justified.

This judgment marked a constitutional reinterpretation, bringing greater transparency into what had previously been an opaque legal framework.

g. Way Forward – Balancing Security with Justice

Scholars, commissions, and civil society have proposed reforms that balance operational needs with constitutional morality:

- **Gradual Repeal**: Withdraw AFSPA in stabilised regions, as already done in Tripura, Meghalaya, and much of Assam.
- **Civilian Complaints Cells**: Establish independent oversight mechanisms with statutory authority.
- **Mandatory Reviews**: Conduct bi-annual evaluations of disturbed area status with active local participation.
- **Human Rights Training**: Institutionalise modules on proportional force, rule of law, and community sensitivity for armed forces.
- **Strengthen Civil Policing**: Build capacities of state police and Central Armed Police Forces (CAPFs) to eventually replace the Army in law-and-order functions.

As one human rights activist argued: *"In a democracy, security must not come at the cost of dignity. Laws like AFSPA must protect the nation without silencing its people."*

Conclusion

AFSPA remains one of India's most debated internal security laws. While it is credited with enabling counter-insurgency stability in Jammu and Kashmir and the Northeast, its prolonged application has generated deep alienation, allegations of rights violations, and mounting international criticism.

The future of AFSPA must be conditional, tied to periodic reviews, and linked with the strengthening of civilian institutions. As one observer succinctly noted: *"Security without accountability breeds alienation; accountability without security breeds instability."*

The AFSPA debate highlights the central dilemma of internal security: extraordinary powers may be necessary in conflict zones, but unchecked authority erodes legitimacy and trust. In the digital era, this very tension resurfaces in new arenas—surveillance, data collection, and monitoring of

communication networks. As India expands its use of tools like call interception, facial recognition, CCTV grids, and internet shutdowns, the challenge is no longer limited to insurgency areas. It now extends to the daily lives of ordinary citizens, raising pressing questions of privacy, freedom of expression, and the limits of state power.

The next section examines this contemporary debate on surveillance versus privacy—a defining theme for democratic security in the twenty-first century.

12.2 Surveillance vs Privacy

a. Introduction

In the digital era, surveillance has emerged as a core instrument of national security. From intercepting communications to scanning social media, modern surveillance tools enable governments to pre-empt terror attacks, track organised crime networks, monitor radicalisation pipelines, and counter espionage.

India has invested heavily in technological systems such as the Centralised Monitoring System (CMS), NATGRID, and keyword-based internet filters like NETRA. More recently, revelations around Pegasus spyware brought global attention to the secretive world of digital monitoring.

Yet these expanded capabilities raise profound constitutional and ethical dilemmas. Without robust safeguards, surveillance can turn into indiscriminate data collection—eroding the citizen's right to privacy, creating a chilling effect on free speech, and opening doors to political misuse.

The Supreme Court's landmark judgment in *K.S. Puttaswamy vs Union of India* (2017) recognised privacy as a fundamental right under Article 21, laying down strict tests of legality, necessity, and proportionality. The Court made clear that the question is not whether surveillance is required—it certainly is—but whether it can be made accountable, lawful, and proportionate in a democracy.

As one Bench observed during the Pegasus hearings: *"The State cannot get a free pass every time the spectre of national security is raised."*

b. The Core Dilemma

Surveillance is considered essential for:

- Pre-empting terror strikes and major security incidents.
- Detecting sleeper cells and radicalisation pipelines.
- Tracking narcotics, arms trafficking, and espionage networks.

But it often suffers from systemic weaknesses:

- Lack of transparency and legal clarity.
- Mass, untargeted data collection.
- Potential misuse for political surveillance.
- Chilling effects on dissent and freedom of expression.

Thus, while surveillance may protect the State, unchecked it risks undermining the very citizens it seeks to safeguard.

c. Major Surveillance Mechanisms in India

- **Pegasus Spyware**: A military-grade spyware capable of infiltrating phones through "zero-click" exploits. Its alleged use against journalists, opposition leaders, and activists in India triggered global outrage over unauthorised surveillance.

- **Centralised Monitoring System (CMS)**: A pan-India platform enabling real-time interception of calls, SMS, emails, and internet traffic. Critics highlight the absence of parliamentary or judicial oversight.
- **NATGRID (National Intelligence Grid)**: Integrates 21 critical datasets—from banking and telecom to travel records—accessible to 10 central agencies. While powerful, it raises concerns of profiling and potential data leaks.
- **NETRA (Network Traffic Analysis)**: An intelligence system that scans the internet for keywords such as "bomb" or "attack." It has been criticised for indiscriminate sweeps and false positives.
- **Social Media Monitoring Cells**: Units that track Twitter, Facebook, Telegram, and other platforms for extremist content. However, they have sometimes been accused of targeting satire, dissent, or legitimate political criticism.

d. The Pegasus Controversy (2021)

- A leaked database of 50,000 phone numbers revealed global targeting by NSO Group's Pegasus spyware.
- In India, potential targets included journalists, Supreme Court judges, opposition leaders, and civil society activists.
- The Government neither confirmed nor denied its use, citing national security.
- The Supreme Court appointed a technical committee, which detected malware traces but reported lack of cooperation from authorities.
- The Court emphasised that even in matters of national security, executive claims cannot override fundamental rights without scrutiny.

e. Legal Framework for Surveillance in India

India's surveillance powers currently rest on a patchwork of colonial and digital-era laws:

- **Indian Telegraph Act, 1885 – Section 5(2)**: Allows interception of telephonic communications during public emergencies or in the interest of public safety.
- **Information Technology Act, 2000 – Section 69**: Permits decryption and monitoring of digital communications with written approval from the Home Secretary.
- **Supporting Rules**: Telegraph Rules and IT Rules (2009) prescribe procedures for authorisation and record-keeping.

Gaps in the Framework:

- No dedicated surveillance law tailored to the digital age.
- Absence of parliamentary or independent oversight (unlike the United States with FISA courts or the United Kingdom with the Investigatory Powers Act).
- Citizens lack the right to be informed or to challenge interception orders.
- Approval remains executive-driven, with little scope for judicial pre-approval.

f. Puttaswamy Judgment (2017) – Right to Privacy

A nine-judge Constitution Bench of the Supreme Court unanimously held that privacy is a fundamental right, intrinsic to personal dignity, autonomy, and liberty.

The Court laid down a three-part test for any state action limiting privacy:

- **Legality**: A valid legal basis must exist.
- **Necessity**: The action must serve a legitimate state interest.
- **Proportionality**: The means adopted must be the least intrusive available.

The judgment made clear that mass, indiscriminate surveillance without legislative sanction violates constitutional principles. It also underscored the urgent need for a comprehensive data protection regime, placing privacy at the heart of India's democratic framework.

g. Way Forward – Reconciling Security with Liberty

Policy experts and jurists have proposed a reform-oriented path to balance national security needs with individual freedoms:

- **Enact a Surveillance Reform Law**: Introduce clear thresholds for surveillance, judicial pre-approval for interception, and citizen grievance mechanisms.
- **Strengthen Data Protection**: Expedite implementation of the Digital Personal Data Protection Act with strong consent rules, purpose-limitation, and storage safeguards.
- **Parliamentary Oversight**: Create a multi-party standing committee on surveillance, modelled on frameworks in the US and UK.
- **Transparency Reports**: Mandate redacted annual reports from intelligence agencies to ensure limited but meaningful public accountability.
- **Citizen Empowerment**: Provide mechanisms for individuals to challenge illegal interception orders before courts or regulatory bodies.

As one security analyst notes: *"In a democracy, national security must secure rights—not strip them."*

Conclusion

Surveillance is indispensable in the age of terrorism, cybercrime, and disinformation warfare. But unless guided by strong laws, proportional safeguards, and independent oversight, it risks morphing into mass monitoring incompatible with democratic freedoms.

India's path forward must therefore harmonise the twin imperatives of national security and personal liberty, ensuring that its digital shield does not become a digital blindfold.

As of 2023, India continues to rely on the Telegraph Act of 1885 and the IT Act of 2000 for authorising surveillance—laws that predate modern digital realities and lack explicit safeguards for privacy.

The debate on surveillance and privacy highlights the central dilemma of democratic security: how far the State can go in the name of protection before it undermines the very freedoms it seeks to defend. Yet, surveillance represents only one layer of this ethical spectrum. At the sharper edge of counter-terrorism, the dilemmas become even starker—questions of life, liberty, and human dignity in situations of imminent threat.

Counter-terrorism often tests the moral boundaries of a democracy. Should the State detain individuals on suspicion to prevent attacks? Can torture or coercive interrogation ever be justified if it extracts information that could save lives? Where does deterrence end and injustice begin?

The next section explores these fraught issues, focusing on the ethics and legality of preventive detention and torture in counter-terror operations—examining not only their strategic utility but also their moral and constitutional consequences.

12.3 Ethics of Counter-Terrorism: Torture and Preventive Detention

a. Context: Balancing Liberty and Security

Counter-terrorism is one of the most difficult terrains for a democracy, situated at the uneasy intersection of national security imperatives and constitutional morality. Faced with unpredictable, high-impact threats such as terrorism, insurgency, and hybrid warfare, the State often invokes extraordinary measures—ranging from coercive interrogation to preventive detention—to pre-empt attacks and gather actionable intelligence.

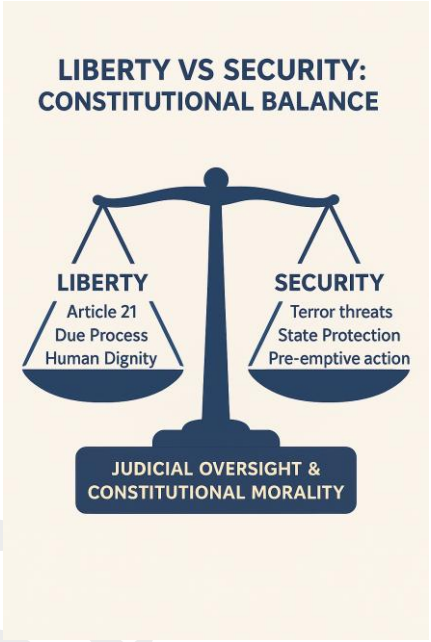
These measures, however, come at a steep cost. Torture erodes the rule of law, delegitimises institutions, and violates human dignity. Preventive detention, when misused, can become an instrument of political suppression rather than a shield against genuine threats.

The challenge before India is not whether the State should act—it must—but how it acts, ensuring that in defending sovereignty it does not corrode the moral foundations of the Republic. As Nietzsche warned: *"In fighting monsters, we must take care not to become one."*

b. Torture in Counter-Terrorism: The Ethical Dilemma

Rationale for Use:

- Extracting intelligence quickly from terror suspects.
- The "ticking time bomb" argument, which claims extreme measures are justified to prevent imminent mass casualties.
- Deterrence, by instilling fear of harsh consequences among potential militants.



Ethical and Legal Problems:

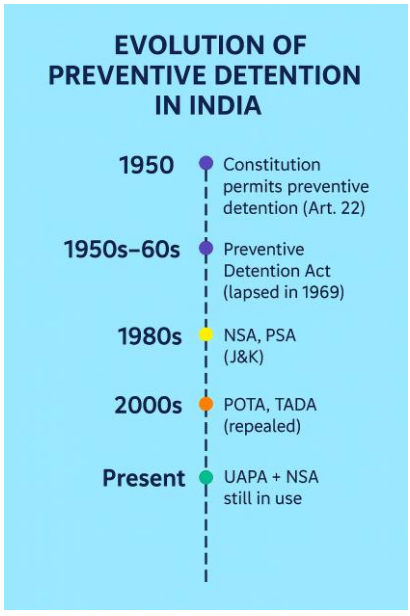
- **Human Rights**: Torture violates Article 21 of the Constitution and contravenes India's obligations under the UN Convention Against Torture (signed in 1997, yet to be ratified).
- **Rule of Law**: It undermines due process and the presumption of innocence.
- **Effectiveness**: Coerced confessions are unreliable; victims often provide false or misleading information.
- **Moral Hazard**: Once normalised, torture legitimises cruelty and corrodes the democratic ethos of security institutions.

Illustrative Cases:

- Allegations of custodial torture during high-profile encounters such as Batla House (2008).
- Global parallels like the CIA's "enhanced interrogation" programme post-9/11 or the Khashoggi killing, which provoked international condemnation.

c. Preventive Detention: Legal Tool versus Ethical Challenge

Constitutional Backing:
Article 22 of the Indian Constitution explicitly provides for preventive detention, allowing detention without trial for up to three months, extendable with approval from an advisory board.



Legislative Instruments in India:

- National Security Act (NSA).
- Unlawful Activities (Prevention) Act (UAPA).
- Jammu and Kashmir Public Safety Act.
- COFEPOSA (Conservation of Foreign Exchange and Prevention of Smuggling Activities Act).

Concerns:

- **Absence of Trial or Evidence**: Detention is based on suspicion rather than conviction.
- **Misuse**: Often deployed against political opponents, minorities, or student activists.
- **Judicial Deference**: Courts have generally deferred to executive discretion in security matters.
- **Violation of Liberty**: Prolonged detentions without trial contradict the spirit of Article 21 and democratic due process.

d. Comparative Global Experiences

Country	Torture	Preventive Detention
United States (post-9/11)	"Enhanced interrogation" at CIA black sites, later discredited	Guantanamo Bay detentions without trial
United Kingdom	Explicit prohibition of torture; strong parliamentary oversight	Extended detention under Terrorism Acts, subject to judicial review
China	Torture allegations in Xinjiang counter-terror campaigns	Indefinite detention of Uighur Muslims under "re-education" camps
India	Custodial deaths remain common; absence of anti-torture law	Preventive detention under UAPA, NSA, and state laws

e. Way Forward: Towards an Ethical Security Framework

- **Ratify the UN Convention Against Torture**: Move from symbolic signature to legal ratification, signalling India's commitment to global norms.
- **Enact an Anti-Torture Law**: Based on the 2017 Law Commission draft, criminalising custodial torture and providing safeguards for accountability.
- **Strengthen Judicial Oversight**: Ensure regular, time-bound reviews of all preventive detention cases by independent boards.
- **Shift to Scientific Investigations**: Rely on forensic science, cyber-tracking, and surveillance technologies rather than coercion.
- **Independent Custodial Death Inquiry Boards**: As recommended by the NHRC and Supreme Court, establish credible institutions for investigating custodial abuses.

Conclusion

India's counter-terrorism posture must be both effective and ethical. Torture is not only immoral but operationally counterproductive, yielding unreliable intelligence and fuelling alienation. Preventive detention, though constitutionally permitted, must be exercised sparingly, under strict safeguards and oversight.

In a democracy, national security must be built on constitutional morality, ensuring that the Republic is defended without compromising the dignity and liberty of its citizens.

"The strength of a democracy is measured not by the power it wields over its enemies, but by the justice it affords to its own citizens."

As of 2023, India remains one of the few large democracies yet to ratify the UN Convention Against Torture, despite having signed it in 1997.

The preceding discussion explored the legal and ethical dilemmas of internal security, from AFSPA and surveillance to preventive detention and torture. These debates reveal a fundamental truth: in a democracy, security is not simply a question of capability, but of legitimacy. The State's power must always be balanced against the rights of citizens and the principles of constitutional morality.

Yet, even as India grapples with these internal debates, the nature of conflict itself is changing. Conventional wars are increasingly rare; adversaries now deploy tools of economic sabotage, cyber intrusions, disinformation campaigns, proxy militias, and deniable operations. These are not open wars but grey-zone conflicts, where the line between peace and war blurs, and the battlefield extends into minds, markets, and digital spaces.

Having examined the legal-ethical foundations of internal security, we now turn to the strategic frontiers of hybrid warfare—understanding how adversaries exploit ambiguity, and how India must respond to threats that are silent, persistent, and multidimensional.

Chapter 13. Hybrid Warfare & Grey-Zone Conflicts

Introduction

Hybrid warfare represents the deliberate fusion of conventional, irregular, cyber, and informational tactics, orchestrated to achieve political, military, and economic objectives without formally crossing the threshold of declared war. Unlike traditional conflict, which unfolds on well-defined battlefields, hybrid warfare thrives in the grey zone—those ambiguous spaces where attribution is difficult, escalation is carefully managed, and adversaries exploit legal loopholes, technological vulnerabilities, and social divisions to weaken their opponent from within.

For India, hybrid threats are not abstract constructs but lived realities. Pakistan has long relied on proxy terrorism, narco-trafficking, and information warfare in Kashmir, while China has operationalised its "Three Warfares" doctrine—psychological, media, and legal warfare—along the Line of Actual Control and beyond.

India's complex security environment, porous borders, rapid technological transition, and societal diversity provide fertile ground for such tactics.

Why Hybrid Warfare Matters for India:

- Hybrid operations blur the line between war and peace, complicating deterrence and attribution.
- They enable adversaries to inflict strategic damage without overt military confrontation.
- They target not only India's borders but also its political stability, economic growth, and social cohesion.

a. Tools of Hybrid Warfare

i. Lawfare (Legal Warfare)

Law becomes a weapon when adversaries exploit domestic or international legal frameworks to legitimise territorial claims or constrain opponents.

- **Examples**: China's invocation of the "nine-dash line" to assert control over the South China Sea; Pakistan approaching the International Court of Justice in the Kulbhushan Jadhav case.
- **Challenge**: Weaponisation of law undermines neutrality and transforms judicial forums into arenas of strategic contest.

ii. Trade Warfare

Economic instruments can destabilise nations without a single shot being fired.

- **Examples**: The United States–China tariff war; India's post-Galwan restrictions on Chinese apps such as TikTok; China's near-monopoly over rare earth elements.
- **Impact**: Such measures disrupt supply chains, impose economic costs, and shape strategic choices in ways akin to traditional blockades.

iii. Cyber Operations

Cyberspace is the most fluid domain of hybrid conflict, where malware, ransomware, espionage, and denial-of-service attacks can cripple critical infrastructure.

- **Examples**: The WannaCry ransomware attack on financial and health systems; Stuxnet (allegedly developed by the United States and Israel) to disable Iran's nuclear programme.
- **Indian Exposure**: Limited indigenous hardware, vulnerabilities in government endpoints, and increasing reliance on digital platforms. The Zhenhua database, tracking Indian political and defence figures, underscores the risks of cyber-espionage.

iv. Information Warfare

Information manipulation is perhaps the most insidious tool, seeking to influence perception rather than territory.

- **Tactics**: Fake news, deepfakes, social media bot networks, and targeted propaganda campaigns.
- **Examples**: Russian disinformation during the Ukraine war; Pakistan's amplification of anti-India narratives on Kashmir.
- **Impact**: These operations erode trust, polarise societies, and weaken democratic discourse.

v. Narrative Building

Narratives shape legitimacy, and legitimacy shapes power. States and non-state actors alike invest heavily in controlling discourse domestically and globally.

- **Examples**: Russian outlets such as RT, Chinese platforms like CGTN, and cultural diplomacy via Confucius Institutes. In India, global protest narratives—such as those around Palestine or the farmers' movement—have been reframed by adversaries to exert pressure.

b. India's Readiness

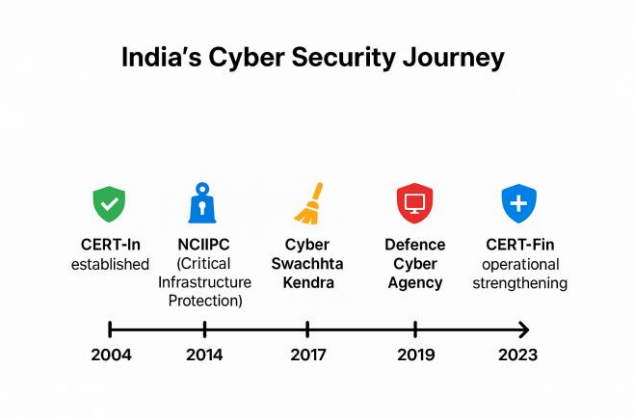
i. Doctrinal Evolution

India has sought to adapt its doctrines to meet hybrid challenges:

- **Cold Start Doctrine**: Envisages rapid mobilisation for limited war under the nuclear threshold.
- **Integrated Battle Groups (IBGs)**: Modular, flexible units designed for swift deployment.
- **Land Warfare Doctrine (2018)**: Stresses multi-domain operations, counter-insurgency, and cyber preparedness.
- **Challenge**: Absence of integrated theatre commands continues to limit real-time joint action, reducing the synergy needed to counter blended threats.

ii. Cyber and Technical Architecture

Several institutional initiatives reflect India's recognition of cyberspace as a battlefield:



- **Defence Cyber Agency (2019)**: Tri-service body responsible for military cyber operations.
- **CERT-In**: Nodal civilian agency for cybersecurity incidents.
- **NCIIPC (National Critical Information Infrastructure Protection Centre)**: Protects assets such as banking networks and power grids.
- **CERT-Fin**: Focused on threats to the financial sector.
- **Cyber Swachhta Kendra**: Designed for botnet cleaning and raising cyber hygiene awareness.

Yet these efforts remain fragmented. India urgently requires a unified cyber command integrating offensive and defensive capacities while coordinating seamlessly between civilian and military stakeholders.

Conclusion

Hybrid warfare has redefined conflict. The battlefield now extends into minds, markets, and machines. For India, the challenge is acute: Pakistan's proxy terror networks, China's cyber-espionage and influence campaigns, and transnational disinformation flows converge to test the resilience of democratic institutions.

Resilience will depend on three pillars:

- Multi-domain integration
- Indigenous technological capability.
- Proactive counter-narratives to neutralise disinformation.

As Sun Tzu observed: *"The supreme art of war is to subdue the enemy without fighting."* Hybrid warfare seeks precisely this. India's task is to master the grey zone before adversaries master it against her.

According to government data, cyberattacks targeting Indian networks increased by over 200% between 2018 and 2022, underscoring how cyberspace has already become the frontline of hybrid conflict.

If hybrid warfare represents the broad architecture of twenty-first-century conflict, drones and unmanned aerial vehicles (UAVs) are among its sharpest tactical instruments. Cheap, deniable, and disruptive, drones epitomise the grey-zone toolkit—capable of smuggling narcotics across Punjab's fields, dropping weapons in Jammu, striking oil facilities in Saudi Arabia, or altering the course of wars in Ukraine and Nagorno-Karabakh.

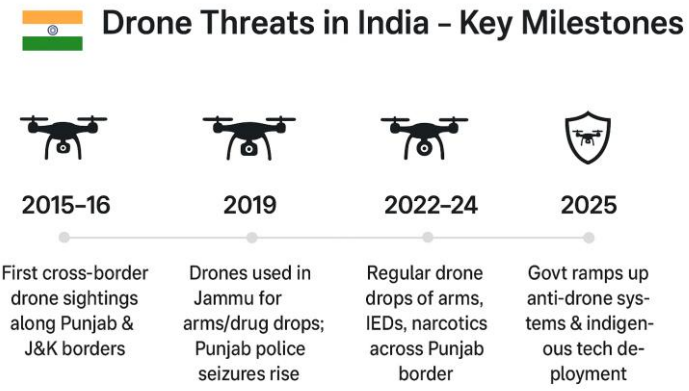
For India, drones encapsulate both opportunity and threat. On the one hand, indigenous UAV programmes enhance surveillance and precision-strike capability. On the other, hostile actors—whether state-backed or insurgent—exploit commercially available drones for infiltration, narco-terrorism, and targeted attacks.

Having explored the theory and practice of hybrid warfare, it is natural to now turn to drones—the most visible and immediate manifestation of this new age of conflict.

Chapter 14. Drone Threats & UAV Warfare

Introduction

Drones, or Unmanned Aerial Vehicles (UAVs), represent one of the most striking illustrations of dual-use technology in the twenty-first century. Initially developed for civilian applications such as agriculture, disaster management, and logistics, they have rapidly been appropriated into the security domain. On modern battlefields, as well as in internal security theatres, drones now act as force multipliers for both state and non-state actors.



For adversaries, UAVs are particularly attractive because they are relatively inexpensive, easily accessible through commercial markets, and inherently deniable. Their adaptability allows them to carry diverse payloads ranging from surveillance equipment and narcotics to explosives and propaganda material. They are also difficult to detect, capable of low-altitude flight, radar evasion, and even autonomous navigation guided by pre-programmed GPS coordinates.

The Jammu Airbase attack of 2021 was a watershed moment for India, marking the first known instance of a drone-based aerial strike on a military facility. Simultaneously, cross-border narco-drone networks in Punjab have fused terrorism with organised crime, demonstrating that UAV threats are not futuristic abstractions but pressing, immediate challenges.

"In the wars of the future, the enemy may never set foot on your soil—yet his shadow will fly over your skies."

a. Drone Incidents: Jammu Airbase and Punjab Drug Drones

i. Jammu Airbase Attack (2021)

The Jammu incident highlighted the vulnerability of strategic installations to small drones. In June 2021, drones carrying improvised explosive devices (IEDs) targeted the technical area of the Jammu Air Force Station.

- The aircraft flew at low altitude, evading conventional radar systems.
- They dropped precision-guided payloads with deniability.
- The strike caused no major damage but carried strategic significance, demonstrating that non-state actors could replicate aerial strike capabilities once reserved for state militaries.

This event expanded India's internal security threat spectrum, proving that UAVs had crossed from peripheral nuisance to central challenge.

ii. Punjab: Drone-Aided Drug and Arms Smuggling

Punjab's border districts—Tarn Taran, Amritsar, Ferozepur, and Gurdaspur—have emerged as hotspots for drone-based smuggling. UAVs launched from across the Pakistan border are routinely used to drop consignments of heroin, small arms, and ammunition.

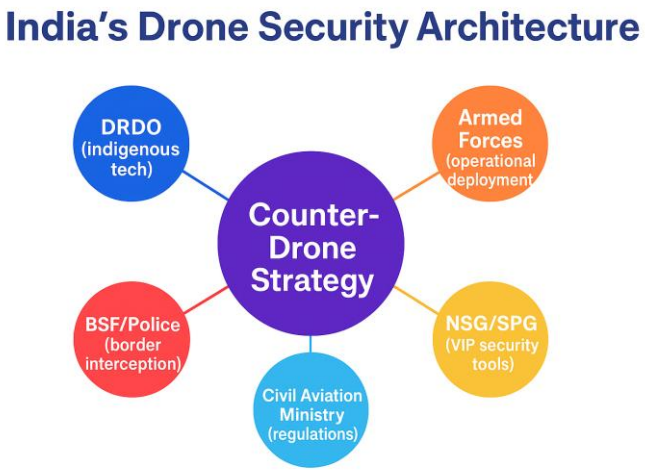
- Data: Over 167 drone sightings near the international border in 2019.
- Impact: These operations have created a dangerous convergence of narcotics trafficking and terrorism, where proceeds from drug sales are funnelled into extremist activities.

This narco-drone nexus represents one of the gravest hybrid threats to India's security.

b. Drone Regulations, 2021

India's regulatory framework for drones has evolved rapidly in response to both commercial opportunities and emerging threats.

- **UAS Rules, 2020**: Imposed heavy compliance burdens, stifling innovation.
- **Drone Rules, 2021**: Replaced UAS Rules with a more enabling framework.



Key Features of the 2021 Rules:

- Abolition of prior security clearance requirements to reduce entry barriers.
- Creation of an interactive digital portal for drone registration and real-time airspace mapping.
- Classification of airspace into green, yellow, and red zones, with most drones permitted freely in green zones.
- Waiver of pilot licensing requirements for micro-drones under two kilograms when used for non-commercial purposes.
- Special windows for start-ups, industry, and academic research to promote indigenous innovation.

This reform reflects the government's attempt to balance technological growth with national security imperatives.

c. Counter-UAV Technology

i. Indigenous Anti-Drone Systems

India has prioritised domestic solutions for neutralising UAV threats. The Defence Research and Development Organisation (DRDO) has developed Directed Energy Weapons (DEWs):

- A 10 kW vehicle-mounted laser system with an effective range of about two kilometres.
- A 2 kW tripod-mounted variant capable of neutralising targets within one kilometre.

These systems offer advantages of precision, silent operation, and minimal collateral damage, though their mass induction into security forces is still pending.

ii. Imported Solutions

India has also turned to foreign technology for urgent operational requirements.

- **SMASH-2000 Plus**: An Israeli electro-optic sight enabling soldiers to shoot down drones using assault rifles with remarkable accuracy. Already deployed with frontline units in sensitive sectors.

iii. Other Counter-UAV Measures

- **RF Jammers and Net Guns**: Used by NSG and SPG for VIP protection.
- **SWATHI Weapon Locating Radar**: Originally for artillery tracking, but adaptable for UAV detection when integrated into surveillance grids.
- **C-DOME (conceptual study)**: Based on Israel's Iron Dome, considered for defending high-value assets against drone swarms.

Conclusion

Drones have transformed the nature of both internal and external security. No longer peripheral gadgets, they have become central instruments of asymmetric warfare. The Jammu airbase attack and Punjab's narco-drone network underscore how UAVs can bypass conventional defences, disrupt stability, and fund terrorism.

India's counter-drone strategy must therefore be multi-layered:

- Detection through radar, radio-frequency sensors, and AI-powered imaging.
- Identification with friend–foe classification mechanisms.
- Neutralisation using DEWs, jammers, and kinetic interceptors.
- Policy and policing with updated regulations, standardised protocols, and inter-agency coordination.

Ultimately, success will depend on indigenising counter-drone technology, integrating civil–military airspace monitoring, and building international cooperation frameworks against UAV-enabled terrorism and organised crime.

Drones encapsulate the paradox of modern security: tools of development that can swiftly become weapons of disruption. The challenge for India is to ensure that the same skies that enable agricultural innovation and emergency relief are not hijacked by adversaries for narco-terror or asymmetric warfare.

The rise of drones and UAVs illustrates how asymmetric tools exploit vulnerabilities in India's security grid, bypassing traditional defences to strike at high-value targets or sustain cross-border crime.

If UAVs embody the vulnerabilities of the skies, India's seaboard symbolises the vulnerabilities of the oceans. With a 7,500-kilometre coastline, 1,200 offshore islands, and critical maritime trade arteries, the nation faces formidable challenges at sea.

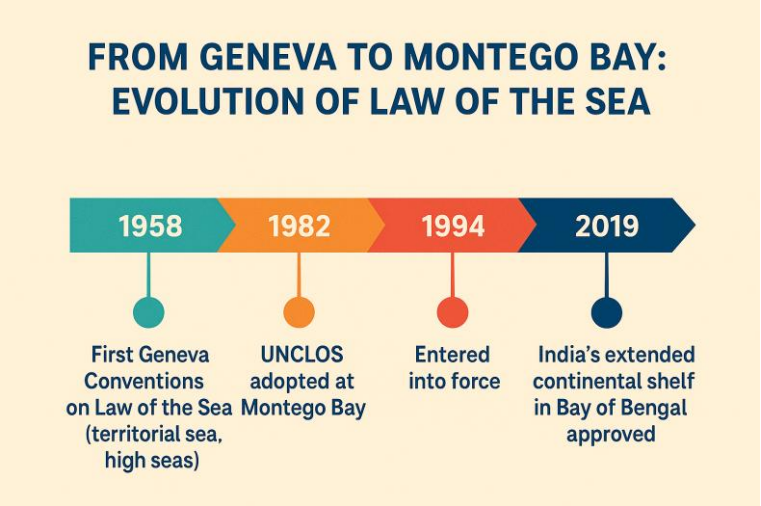
From the 1993 Mumbai blasts, where explosives were smuggled through coastal routes, to the 26/11 attacks, which exposed glaring gaps in coastal surveillance, India has repeatedly learned that maritime insecurity translates directly into national insecurity. At the same time, competition in the Indian Ocean Region (IOR), piracy, and narco-trafficking add external complexities.

Having examined airborne threats, it is therefore natural to turn to the seas. The next chapter explores Maritime and Coastal Security, focusing on protecting India's vast littoral zone and ensuring that its blue economy and strategic ocean spaces remain safe from both conventional and hybrid threats.

Chapter 15. Maritime and Coastal Security

Introduction

India's maritime security is inseparable from its economic vitality and strategic stability. With a coastline of 7,516 kilometres, 1,382 islands, and an Exclusive Economic Zone (EEZ) extending over 2.37 million square kilometres, the maritime domain represents both a vast opportunity and a significant vulnerability.



Over 95% of India's external trade by volume and nearly 80% of crude oil imports transit through the seas, rendering ports, sea lines of communication (SLOCs), and offshore infrastructure strategic lifelines.

However, history demonstrates how lapses in coastal vigilance can translate into devastating consequences:

- The 1993 Mumbai blasts relied on explosives smuggled through porous shores.
- The 26/11 Mumbai terror attacks revealed the dangers of unmonitored fishing vessels and inadequate maritime domain awareness.

In recent years, the spectrum of threats has widened further to include narco-terrorism, piracy, drone-assisted smuggling, and undersea sabotage of cables and pipelines.

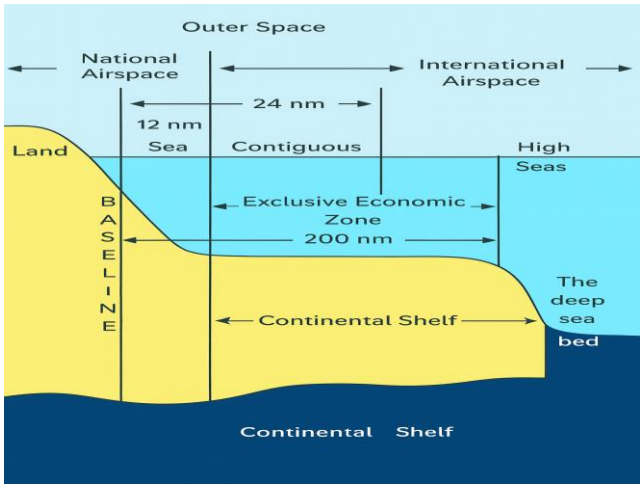
Post-26/11 reforms have brought significant improvements, including the establishment of the National Command, Control, Communication and Intelligence (NC3I) Grid, the Coastal Surveillance Network, Joint Operations Centres, and multi-agency drills such as Sagar Kavach. Yet, challenges remain—technological asymmetries, gaps in undersea domain awareness, and persistent coordination deficits between multiple agencies prevent the creation of a seamless security shield across India's littoral zone.

India's maritime and coastal security strategy must therefore balance hard security measures with port-led development initiatives such as Sagarmala, integrating defence, development, and diplomacy in the maritime space.

15.1 UNCLOS Zones

a. Introduction

The United Nations Convention on the Law of the Sea (UNCLOS), adopted in 1982 and in force since 1994, is widely regarded as the *"constitution of the oceans."* It codifies the rights and obligations of states in maritime spaces, defining zones of jurisdiction, the scope of sovereignty, and the balance between coastal state rights and freedoms enjoyed by other states.



For India, UNCLOS provides the legal framework for protecting sovereignty, ensuring economic rights over marine resources, and safeguarding security interests in the Indian Ocean.

b. Key Maritime Zones under UNCLOS

Zone	Extent from Baseline*	Sovereignty / Rights of Coastal State	Rights of Other States
Internal Waters	Landward of baseline	Full sovereignty, equivalent to land territory	None, without explicit permission
Territorial Sea (TS)	0–12 nautical miles	Full sovereignty; foreign vessels enjoy right of innocent passage	Innocent passage, provided peace and security are not compromised
Contiguous Zone (CZ)	12–24 nautical miles	Enforcement jurisdiction for customs, fiscal, immigration, and sanitary laws	Freedom of navigation and overflight
Exclusive Economic Zone (EEZ)	12–200 nautical miles	Sovereign rights to explore, exploit, conserve, and manage natural resources of the water column and seabed	Freedom of navigation, overflight, and submarine cable-laying
Continental Shelf (CS)	Up to 200 nm, extendable to 350 nm with geological evidence	Sovereign rights over seabed and subsoil resources (not the water column beyond EEZ)	Freedom of navigation and laying pipelines and cables
High Seas	Beyond EEZ	No sovereignty; common heritage of mankind	All states enjoy freedom of navigation, fishing, research, overflight

*Baseline: Normally the low-water line along the coast.

c. India's Maritime Zones (as per Maritime Zones Act, 1976)

- **Internal Waters and Territorial Sea**: Full sovereignty; foreign vessels may exercise innocent passage.
- **Contiguous Zone**: India exercises jurisdiction over customs, fiscal, immigration, and sanitation enforcement.
- **Exclusive Economic Zone (EEZ)**: Nearly 2.37 million sq. km., rich in hydrocarbons, fisheries, and polymetallic nodules.s
- **Continental Shelf**: Extended claims in the Bay of Bengal approved by the UN Commission on the Limits of the Continental Shelf (CLCS) in 2019.

d. Security and Strategic Implications for India

- **Territorial Sea and Contiguous Zone**: Countering arms trafficking, illegal immigration, and narcotics smuggling.
- **EEZ**: Protecting offshore oil and gas platforms, undersea cables, and fisheries from illegal, unreported, and unregulated (IUU) fishing or sabotage.
- **Continental Shelf**: Securing seabed mining and hydrocarbon exploration.

- **High Seas**: Contributing to global maritime stability through anti-piracy patrols, freedom of navigation operations, and cooperative security initiatives.

e. Disputes and Challenges

- **Fisheries Conflicts**: Repeated incidents in the Palk Strait involving Indian and Sri Lankan fishermen.
- **Maritime Boundary Disputes**: Ongoing dispute with Pakistan over Sir Creek; delimitation with Bangladesh resolved in 2014 through international arbitration.
- **Freedom of Navigation Operations (FONOPs)**: U.S. Navy operations in India's EEZ without prior consent have led to diplomatic protests.
- **Chinese Activities**: Frequent presence of Chinese survey ships and PLA Navy movements in India's EEZ raise concerns of surveillance and encirclement.

f. Relevance to Internal and Maritime Security

- **Legal Enforcement**: UNCLOS provides the framework for tackling piracy, terrorism, and trafficking at sea.
- **Economic Security**: EEZ resources underpin India's Blue Economy ambitions, linking energy, food, and industrial security.
- **Maritime Diplomacy**: Adherence to UNCLOS enhances India's credibility as a responsible stakeholder in Indo-Pacific maritime governance.

Conclusion

UNCLOS provides not only the legal foundation for maritime sovereignty but also the strategic architecture for security and economic development. For India, protecting its maritime zones under this framework is essential for sustaining growth and projecting influence in the Indian Ocean.

Challenges such as IUU fishing, piracy, foreign survey missions, and naval intrusions underscore the need for enhanced surveillance, legal preparedness, and proactive diplomacy.

"The law of the sea is not just about borders—it is about protecting the lifelines of a nation."

India's EEZ is nearly two-thirds the size of its landmass, underscoring why maritime security is as much about sovereignty as it is about survival.

While UNCLOS provides the legal scaffolding for India's maritime rights and obligations, translating those rights into practical security is far from automatic. Legal sovereignty over waters, seabed, and resources must be backed by the capacity to safeguard them.

India's vast network of ports, sprawling EEZ, and critical SLOCs are the arteries of its economy—but they are also tempting targets for adversaries, criminals, and non-state actors. Ports can become entry points for contraband, weapons, or terrorists; the EEZ, with its oil rigs and undersea cables, is exposed to sabotage and illegal exploitation; and marine trade routes, which carry the bulk of India's commerce, are vulnerable to piracy, blockades, or hybrid disruptions.

The next section therefore examines the vulnerabilities of ports, the EEZ, and marine routes, situating them within India's internal security framework.

15.2 Vulnerabilities and India's Maritime and Coastal Security Architecture

India's maritime vulnerabilities extend across three interconnected domains—its ports, its vast Exclusive Economic Zone (EEZ), and the critical sea lanes of communication (SLOCs) that sustain its economy. Each represents both a national asset and a potential security liability.

a. Vulnerabilities

i. Ports

India operates 12 major ports under central control and nearly 200 non-major ports managed by state governments and private entities. Collectively, they handle almost 95% of external trade by volume, making them indispensable to economic growth and energy security. Ports such as Mundra, Mumbai, Kandla, Visakhapatnam, and Chennai serve as critical nodes in global supply chains.

Key Security Concerns:

- Container security gaps enabling the smuggling of arms and narcotics.
- Insider threats and port mafia networks exploiting systemic weaknesses for cargo theft or collusion with smugglers.
- Cybersecurity vulnerabilities targeting port operating systems, which increasingly rely on digital platforms.

Illustrative Case: In 2021, nearly 3,000 kilograms of heroin were seized at Mundra Port, exposing the nexus between narcotics trafficking and port security vulnerabilities.

ii. Exclusive Economic Zone (EEZ)

India's 2.3 million sq. km. EEZ, extending 200 nautical miles from its baseline, is rich in oil, gas, fisheries, and seabed minerals. However, it faces persistent threats:

- Illegal, Unreported, and Unregulated (IUU) Fishing depleting marine biodiversity and threatening livelihoods.
- Intrusion by Foreign Survey Ships conducting covert espionage or hydrographic missions.
- Undersea Sabotage of oil rigs, pipelines, and communication cables, capable of paralysing energy and digital connectivity.

A core challenge remains India's low patrol density and undersea domain awareness (UDSA) deficit, which hinder real-time detection of sub-surface threats.

iii. Marine Routes (Sea Lines of Communication – SLOCs)

India is strategically positioned near vital chokepoints such as the Strait of Hormuz, Strait of Malacca, and Gulf of Aden. These routes are indispensable for:

- Crude oil imports (India depends on imports for nearly 80% of its crude needs).
- Container shipping routes linking Asia, Africa, and Europe.
- Strategic logistics during crises.

Risks to SLOCs:

- Piracy, particularly in the Gulf of Aden, where Indian naval patrols have frequently intervened.
- Terror infiltration, most starkly revealed during the 26/11 Mumbai attacks.
- Sub-sea sabotage, including deliberate disruption of pipelines and undersea communication cables.

Sagarmala Project

The Sagarmala Project, launched by the Ministry of Ports, Shipping and Waterways, is India's flagship port-led development initiative.

Objectives:

- Modernising port infrastructure.
- Establishing coastal economic zones.
- Improving multimodal connectivity between ports, rail, and roads.
- Facilitating domestic and international trade.

From a security perspective, Sagarmala enhances surveillance and response mechanisms at high-traffic nodes, ensuring that development is integrated with resilience against asymmetric threats.

Deep Sea Fishing (DSF)

Overfishing in shallow waters has led to recurring conflicts in the Palk Bay between Indian and Sri Lankan fishermen. Deep Sea Fishing offers a sustainable solution by shifting pressure away from near-shore ecosystems.

Advantages of DSF:

- Reduces stress on shallow-water ecosystems and prevents illegal poaching.
- Boosts seafood exports and generates employment opportunities.
- Enhances security through GPS, Automatic Identification Systems (AIS), and RFID tagging of DSF vessels, reducing vulnerabilities to smuggling and infiltration.

b. The 26/11 Lessons

The 26/11 terror attacks epitomised the dangers of unmonitored maritime routes. Ten terrorists infiltrated Mumbai by sea using the hijacked trawler MV Kuber, landing undetected at Colaba. Armed with AK-47s and explosives, they inflicted mass casualties, exposing a total collapse in coastal surveillance and inter-agency coordination.

Post-26/11 Reforms:

- **Joint Operations Centres (JOCs):** Established under the Navy in Mumbai, Kochi, and Visakhapatnam for integrated command.
- **Coastal Surveillance Network (CSN):** Deployment of radars, Automatic Identification Systems (AIS), Vessel Traffic Management Systems (VTMS), and long-range cameras along the coast.
- **NC3I Grid:** A centralised platform integrating data from radars, police, ports, and fishing units.
- **Fishermen Involvement:** Biometric ID cards, RFID tagging of vessels, and distress alert transmitters issued to coastal communities.
- **Mock Drills:** Regular exercises such as Sagar Kavach and Sea Vigil to test coordination among multiple agencies.

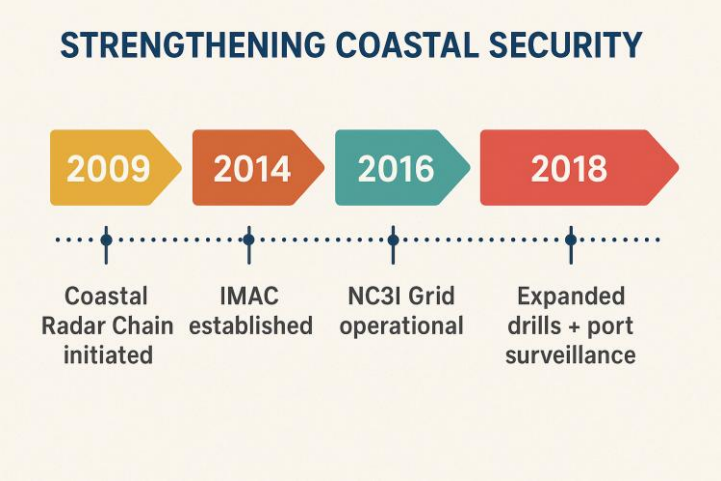
Collectively, these reforms shifted India's security orientation from a land-border mindset to a coast-centric, intelligence-led maritime security approach.

c. India's Maritime and Coastal Security Architecture: Institutions, Intelligence, and the Way Forward

i. Indian Coast Guard (ICG)

Established in 1977 under the Coast Guard Act and placed under the Ministry of Defence, the ICG has jurisdiction across the EEZ up to 200 nautical miles. With a fleet of about 150 vessels and 60 aircraft, its functions include:

- Anti-smuggling and anti-poaching enforcement.
- Search and Rescue (SAR) operations.
- Maritime pollution control and environmental protection.
- Boundary patrols and joint operations with the Navy.



The ICG has been instrumental in seizing narcotics-laden vessels off Gujarat and Tamil Nadu coasts, underscoring its frontline role against maritime crime.

ii. Directorate General (DG) Shipping

As the maritime regulatory authority under the Ministry of Ports, Shipping and Waterways, the DG Shipping is responsible for:

- Ship registration.
- Training of seafarers.
- Enforcement of marine safety codes.

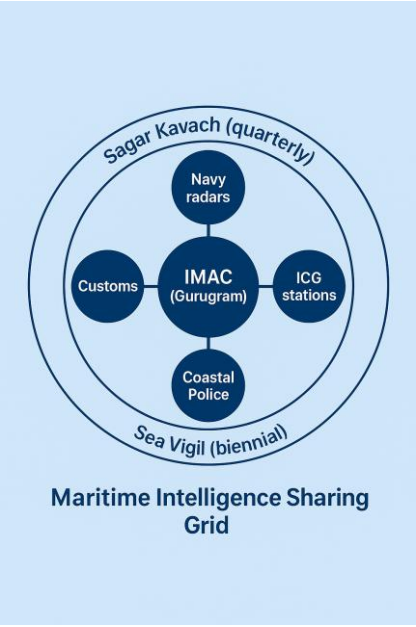
It plays a pivotal role in ensuring India's compliance with the International Maritime Organization (IMO), safeguarding trade, and preventing maritime accidents.

iii. Intelligence-Sharing Mechanisms

India has progressively built multi-layered maritime intelligence structures:

- **NC3I Grid:** Integrates radar data from the Navy, Coast Guard, Customs, and state police.
- **Information Management and Analysis Centre (IMAC):** The central hub for maritime data processing and real-time decision-making.
- **Sagar Kavach:** A quarterly multi-agency coastal security exercise.
- **Sea Vigil:** A biennial nationwide drill involving 13 coastal states and 2 Union Territories.

These mechanisms have improved situational awareness and fostered greater synergy among central and state stakeholders.



Maritime Intelligence Sharing Grid

d. Gaps in Maritime Security

Despite reforms, significant gaps persist in India's maritime security grid:

- **Fishermen Integration:** Biometric tagging remains incomplete. Drones, RFID, and mobile apps could enable real-time geo-tracking of fishing vessels.
- **Undersea Domain Awareness (UDSA):** Still minimal. Investment in sonar nets, seabed sensor arrays, and unmanned underwater vehicles (UUVs) is critical.
- **Fragmented Intelligence:** Weakens coordinated responses. A permanent Maritime Intelligence Fusion Cell is needed to centralise threat analysis.
- **Coastal Policing:** Coastal police remain undertrained and under-equipped. Regular training, technology upgrades, and joint drills with the Navy and Coast Guard are essential.

Conclusion

Maritime and coastal security can no longer be viewed narrowly as naval warfare or anti-piracy patrols. It demands multi-domain preparedness—covering ports, EEZs, SLOCs, deep-sea fishing, and undersea infrastructure.

The way forward lies in:

- Integrating sensors, shooters, and decision-makers through AI-driven Maritime Domain Awareness (MDA).
- Expanding undersea surveillance capabilities with UUVs and seabed sensors.
- Institutionalising community-based vigilance through biometric tagging and digital tools for fishermen.
- Establishing a permanent Maritime Intelligence Fusion Cell for real-time coordination.

Ultimately, India's ability to *"Think Blue, Act Blue"* will decide whether its seas remain a corridor of prosperity or a frontier of insecurity.

"Control of the sea means security; control of the sea means peace; control of the sea means victory." – Alfred Thayer Mahan

India's EEZ is larger than the combined land area of Rajasthan, Madhya Pradesh, and Maharashtra—underscoring why maritime security is not optional but existential.

Having examined the challenges of maritime and coastal security—focused on safeguarding India's EEZ, SLOCs, and littoral communities—it becomes evident that national security cannot be confined to territorial waters or even terrestrial borders.

Just as the seas emerged as the new frontier in the twentieth century, the twenty-first century is witnessing the rise of outer space and emerging technologies as decisive arenas of power and vulnerability.

Space-based assets underpin navigation, communication, surveillance, weather forecasting, and disaster management. Meanwhile, emerging technologies like Artificial Intelligence (AI), quantum computing, drones, and cyber warfare tools are transforming the speed, scale, and complexity of conflict.

Thus, while maritime security highlighted the importance of multi-agency synergy and technological integration in the physical domain, the next chapter turns to Space and Emerging Technology Security—where India must not only defend its strategic assets but also proactively harness innovation to ensure strategic autonomy in a rapidly changing global order.

Chapter 16. Space and Emerging Technology Security

Introduction

Space has shifted from being the *"final frontier"* of exploration to the fifth domain of warfare, alongside land, sea, air, and cyberspace. What began as a Cold War prestige race between the United States and the Soviet Union has now become an arena where satellites underpin almost every facet of modern power—navigation, communication, intelligence, disaster response, and economic infrastructure.

This dependence has created new vulnerabilities. Attacks on satellites, jamming of communications, or the disruption of navigation systems could paralyse military operations, cripple economies, and undermine civilian life. The global shift from the militarisation of space (use of satellites for military support) to the weaponisation of space (deployment of offensive and defensive weapons in space) marks a profound strategic transformation.

The 2007 Chinese anti-satellite (ASAT) test and India's Mission Shakti (2019) underscored that space is no longer a sanctuary. As the United States establishes its Space Force, China expands its Strategic Support Force, and Russia operationalises space warfare units, competition in this new battlespace is accelerating. For India, the challenge is to balance deterrence and strategic autonomy with adherence to global norms, while safeguarding a rapidly growing constellation of civilian and military satellites.

a. Weaponisation of Space and ASAT Tests

i. Understanding Weaponization

Weaponisation refers to the placement or deployment of offensive or defensive weapons in outer space. These may include:

- **Kinetic Weapons**: Missiles designed to destroy satellites.
- **Directed Energy Weapons (DEWs)**: High-powered lasers capable of blinding or disabling satellite sensors.
- **Electronic Warfare (EW) Tools**: Systems that jam or spoof satellite communications.
- **Cyber Capabilities**: Techniques to hack or cripple satellite control systems.

ii. Historical Context

The Cold War planted the seeds of this competition with programmes such as:

- The Soviet Union's Radar Ocean Reconnaissance Satellites (RORSAT).
- The United States' Strategic Defense Initiative (SDI or "Star Wars").

After a period of restraint, China's 2007 ASAT test—which destroyed one of its own weather satellites at 865 km altitude—revived fears of an arms race in space. It also highlighted the extreme vulnerability of satellites in Low Earth Orbit (LEO).

b. Why Countries Pursue Space Weaponisation

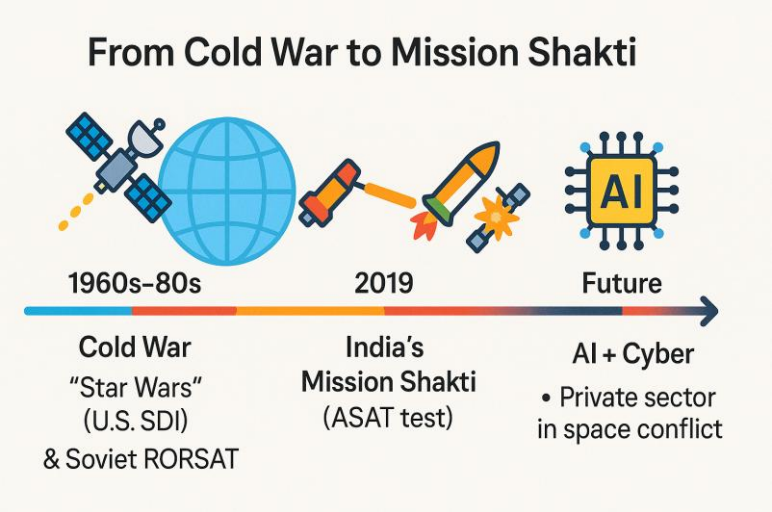
Several factors explain why states are drawn toward weaponisation of space:

- **Military Superiority**
  Space assets are central to modern warfare. From precision-guided munitions using GPS to Intelligence, Surveillance, and Reconnaissance (ISR) satellites, space enables battlefield dominance. Neutralising adversary satellites denies them these advantages.
- **Deterrence and Power Projection**
  Possession of ASAT capabilities creates psychological deterrence, signalling that strikes on satellites—or aggression in another domain—can be met with reciprocal or pre-emptive responses.
- **Space as a Future Battlefield**
  With the creation of the U.S. Space Force and China's Strategic Support Force, space is increasingly seen as the decisive *"high ground"* of future conflicts.
- **Dual-Use Technology**
  Many space technologies serve both civilian and military purposes. For instance, China's BeiDou Navigation Satellite System is used for commercial navigation and secure military logistics.
- **Protection of National Assets**
  With economies and militaries deeply reliant on satellites, states justify defensive weaponisation as insurance. Disabling GPS or communication satellites could paralyse financial systems, transport, and defence preparedness.

c. India's Anti-Satellite Capability: Mission Shakti

i. Mission Shakti

India entered the exclusive club of space powers in March 2019 with Mission Shakti, an ASAT demonstration conducted by the Defence Research and Development Organisation (DRDO).



- **Operation:** A modified interceptor missile from India's Ballistic Missile Defence (BMD) programme successfully destroyed a live Indian satellite in Low Earth Orbit at around 300 km altitude.
- **Outcome:** India became the fourth country—after the United States, Russia, and China—to demonstrate proven ASAT capability.

ii. Strategic Significance

- **Deterrence**: Mission Shakti signalled India's ability to defend its satellites and respond to aggression in space.
- **Strategic Autonomy**: The test reduced India's dependence on foreign partners for defence-related space intelligence.
- **Symbolic Assertion**: It extended India's doctrine of credible minimum deterrence into the space domain.

iii. Complementary Measures

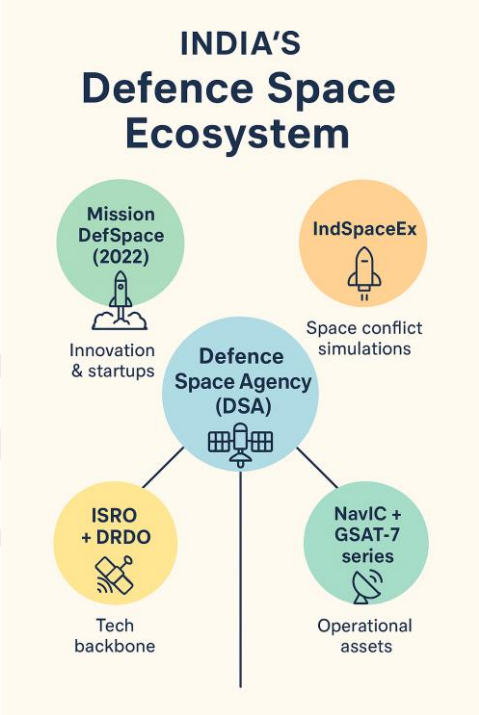
- **Defence Space Agency (DSA):** Established to coordinate space warfare activities across the Army, Navy, and Air Force.

- **Mission DefSpace (2022):** Designed to foster private and academic innovation in military space technologies.
- **IndSpaceEx:** A tabletop exercise simulating conflict scenarios in outer space to refine strategic responses.

Together, these initiatives mark the beginning of India's transition from a passive user of space to an active shaper of its security dynamics.

d. Implications of Space Weaponisation

The weaponisation of space is not merely a technological development—it carries profound global and national implications. The consequences of a single ASAT strike extend beyond military calculations into environmental sustainability, global governance, and civilian life.



i. Global Implications

- **Kessler Syndrome:** A chain reaction of debris collisions could render Low Earth Orbit unusable for decades, crippling satellite infrastructure that underpins global commerce and communications.
- **Violation of Global Norms:** ASAT tests undermine the spirit of the Outer Space Treaty (OST), which envisions space as a domain reserved for peaceful purposes.
- **Strategic Destabilisation:** Space weapons lower the threshold for full-spectrum conflict, as one strike on a critical satellite could escalate into wider hostilities.
- **Civilian Vulnerability:** Systems of global navigation, meteorology, disaster management, and telecommunications—all reliant on satellites—risk collateral damage.
- **Proliferation Pressures:** Demonstrations of counter-space capabilities compel other states to follow suit, creating a spiralling arms race in orbit.

ii. Implications for India

- **Strategic Balance:** India must reconcile the need for credible deterrence with its diplomatic posture as a supporter of the peaceful use of outer space.
- **Asset Vulnerability:** Indian satellites, particularly those in low Earth and geostationary orbits, remain exposed unless shielded with redundancy, resilience, and active defences.
- **Capability Gaps:** A robust Space Situational Awareness (SSA) system, advanced debris tracking networks, and strong cyber protection for ground stations are indispensable for security.

e. Global Treaties: OST and PPWT

i. Outer Space Treaty (OST), 1967

Often described as the *"Magna Carta of space law"*, the OST codified the principle of space as a global commons.

Key Provisions:

- Prohibits placement of nuclear or other weapons of mass destruction in orbit or on celestial bodies.
- Establishes space as *res communis*, not subject to national sovereignty.

- Holds nations responsible for damage caused by their space objects.

Limitations:

- Does not restrict deployment of conventional weapons in space.
- Lacks verification or enforcement mechanisms.
- Ignores threats posed by non-state actors and cyber operations.

ii. Prevention of the Placement of Weapons in Outer Space (PPWT)

Proposed by China and Russia in 2008, the PPWT sought to expand the OST's peaceful-use doctrine.

Key Proposals:

- Prohibition on placing weapons of any kind in space.
- Ban on the use or threat of force against space objects.
- Provisions for verification and compliance.

Criticisms:

- Difficulty distinguishing dual-use satellites from military ones.
- Weak and contested verification mechanisms.
- Western states argue it may freeze kinetic weapons while leaving loopholes for cyber or electronic warfare tools.

India's Position: Broadly supportive of the PPWT's objectives but insists on consensus-based multilateral mechanisms with robust verification regimes.

f. Space as the Fifth Battlefield

i. Why Space Is Central to Modern Warfare

- **Communication:** Secure satellite channels such as the GSAT-7 series for the Indian Navy.
- **Navigation:** Satellite-guided missiles, drones, and UAVs relying on NavIC and GPS.
- **ISR (Intelligence, Surveillance, Reconnaissance):** Satellites like Cartosat and RISAT track troop concentrations and infiltration routes.
- **Cyber-Attack Vector:** Ground stations and control nodes remain vulnerable to hacking and spoofing.
- **AI Integration:** Artificial intelligence enables near real-time targeting and battle management using fused satellite data.

ii. Current Trends

- **Global Militarisation:** The U.S. Space Force, China's Strategic Support Force (SSF), and Russia's Cosmos Troops institutionalise space warfare.
- **Private Players:** Companies such as Starlink, Planet Labs, and BlackSky operate dual-use constellations rivaling state capacities.

iii. India's Priorities

- Upgrading Space Situational Awareness (SSA) to track both natural and hostile threats.
- Developing resilient constellations with redundancy and rapid-launch backup capacity.
- Investing in space cyber-security, ground station hardening, and debris-mitigation technologies.

Conclusion

The coming decades will decide whether outer space remains a global commons for peaceful exploration or descends into a contested, debris-ridden battlefield.

For India, space security demands a multi-layered strategy:

- Deterrence: Maintain credible ASAT and counter-space capabilities.
- Defence: Harden satellites, build redundancies, and enhance cyber resilience.
- Diplomacy: Advocate stronger, verifiable international space security norms.
- Debris Mitigation: Invest in advanced tracking, removal, and collision-avoidance technologies.

Ultimately, dominance in space will depend not on who can destroy satellites, but on who can protect, sustain, and reconstitute them under attack.

"Whoever controls space controls the destiny of Earth." – Lyndon B. Johnson

India's EEZ covers 2.3 million sq. km., but its space domain responsibilities extend far beyond Earth's surface—into the orbits that power its economy, defence, and governance.

The last chapters have shown how India grapples with internal and emerging threats—drones, cyber intrusions, and space weaponisation. Yet, these threats cannot be addressed in isolation.

The twenty-first century has witnessed the rise of overlapping global security frameworks that attempt to regulate or stabilise such challenges. Piracy off Somalia impacts Indian shipping, cyberattacks ripple across borders, and space debris created by one power endangers satellites of all others. But these mechanisms often lag behind the pace of hybrid, transnational threats.

For India, navigating this global security architecture is not just about protecting national interests—it is about shaping the very rules of governance in line with its aspirations as a leading power.

The next chapter therefore explores the Global Security Architecture—its evolution, institutions, gaps, and the role India must play within it.

Chapter 17. Global Security Architecture

Introduction

In the twenty-first century, the very idea of national security has been transformed. Terror financing networks move money across borders in seconds, cyberattacks originate from anonymous servers scattered across continents, and hybrid conflicts blur the line between domestic and external threats.

No state, however powerful, can insulate itself from such interconnected risks. This has necessitated the gradual evolution of a global security architecture—a web of international institutions, conventions, treaties, and bilateral or multilateral frameworks designed to regulate, monitor, and respond to security challenges that transcend frontiers.

For India, active engagement with this architecture is both a necessity and an opportunity. As a rising power and responsible regional actor, India leverages these platforms to counter cross-border terrorism, disrupt money-laundering networks, enhance cyber defence, and shape emerging norms of global security governance.

a. FATF, UNCTC, and INTERPOL

Organisation	Role & Functions	India's Engagement
FATF (Financial Action Task Force)	Global watchdog on money laundering and terror financing. Issues the "Grey List" and "Black List". Develops 40+ Recommendations to guide member states.	India became a full member in 2010. It has consistently used FATF forums to push for stricter scrutiny of Pakistan, contributing to its repeated grey-listing for non-compliance.
UNCTC (UN Counter-Terrorism Committee)	Established under UNSC Resolution 1373 after 9/11. Coordinates implementation of counter-terrorism laws, sanctions, and best practices.	India has been an active supporter, participating in the 2006 Global Counter-Terrorism Strategy and backing the creation of the UN Office of Counter-Terrorism (UNOCT).
INTERPOL	Facilitates cross-border police cooperation through criminal databases, Red/Blue Notices, and coordinated operations.	India frequently uses Red Notices to track fugitives abroad, including economic offenders. It also collaborates on cybercrime through INTERPOL's Global Complex for Innovation in Singapore.

b. The Budapest Convention on Cybercrime

The Budapest Convention, adopted in 2001 under the Council of Europe, remains the only binding international treaty on cybercrime. It seeks to harmonise national laws, improve investigative

techniques, and enable faster cross-border cooperation in crimes such as hacking, fraud, child pornography, and intellectual property violations.

- **Global Acceptance:** As of 2024, more than 75 countries are parties to the convention.
- **India's Position:** India has refrained from signing, citing its non-inclusive drafting process, lack of consideration for developing-country perspectives, and concerns about sovereignty in data governance. Instead, India prefers bilateral arrangements such as Mutual Legal Assistance Treaties (MLATs).

Yet, India's caution has costs. Cybercrime is inherently transnational, and without a global multilateral framework India risks slower access to evidence and weaker deterrence. A future recalibration may require India to balance sovereignty concerns with the pragmatic need for faster international cooperation in tackling digital threats.

c. India's Bilateral Security Partnerships

In addition to multilateral forums, India strategically leverages bilateral partnerships to access advanced technology, intelligence, and operational expertise.

i. Indo–US Security Cooperation

- **Defence:** Foundational agreements such as LEMOA (2016), COMCASA (2018), and BECA (2020) enhance interoperability, secure communications, and geospatial intelligence sharing.
- **Counter-Terrorism:** Joint working groups and intelligence-sharing mechanisms were strengthened post-26/11.
- **Cybersecurity:** The US–India Cyber Dialogue (initiated in 2001) facilitates cooperation in cyber norms and infrastructure defence.

ii. Indo–Israel Cooperation

- **Defence Technology:** India has procured Spike missiles, Phalcon AWACS, and Heron UAVs, making Israel a major defence supplier.
- **Cyber and Intelligence:** Strong collaboration exists in cyber defence, surveillance systems, and border management technologies.
- **Homeland Security:** MoUs include joint training for anti-terror units, urban policing, and disaster preparedness.

iii. Indo–France Cooperation

- **Defence:** Acquisition of Rafale fighters and joint exercises such as Varuna, Shakti, and Garuda enhance military synergy.
- **Counter-Terrorism:** Deepened collaboration after the 2015 Paris attacks, including intelligence exchange.
- **Cybersecurity:** A 2018 MoU institutionalised cooperation on digital regulation, data protection, and cyber defence.

These partnerships reflect India's doctrine of strategic diversification—avoiding overdependence on any single bloc while building resilience through multiple channels.

Conclusion

The global security architecture has moved beyond isolated treaties into an intricate web of overlapping norms, institutions, and partnerships. Yet, it remains fragile, often struggling to keep pace with the borderless nature of twenty-first-century threats.

For India, the path ahead involves:

- Using FATF to choke terror finance and narco-money flows.
- Strengthening global counter-terror norms through UNCTC.
- Leveraging INTERPOL for fugitive tracking and cybercrime enforcement.
- Entering selective bilateral MoUs to access advanced defence and cyber capabilities.

At the same time, India must guard its strategic autonomy, avoid overdependence, and champion inclusive multilateralism that reflects the voices of developing countries.

"Security today is indivisible—no nation is safe until all are safe." – Adapted from the UN Security Doctrine

According to the Ministry of External Affairs, India is now part of over 45 bilateral and multilateral security arrangements, underscoring its transformation from a passive rule-taker to an active rule-shaper in global security governance.

If global institutions like the United Nations, FATF, and INTERPOL define the rules of traditional security, the digital domain is rapidly emerging as the new frontier where sovereignty, security, and governance collide.

Unlike borders on land or sea, the internet knows no geography—yet its infrastructure, platforms, and data flows are controlled by states, corporations, and transnational networks that often operate beyond the reach of conventional treaties.

For India, this creates both opportunities and vulnerabilities. On one hand, digital platforms enable economic growth, e-governance, and citizen empowerment. On the other, dependence on foreign servers, unregulated cross-border data flows, and absence of a global consensus on cyber norms raise critical questions of digital sovereignty.

Just as space became the "fifth battlefield," cyberspace has become the "sixth arena" where power is projected, narratives are contested, and security is negotiated.

The next chapter therefore turns to Internet Governance and Data Sovereignty—a domain that will define not only the architecture of global security but also the very contours of national autonomy in the information age.

Chapter 18. Internet Governance & Data Sovereignty

Introduction

In the twenty-first century, data has assumed the status of a strategic resource—often described as the *"new oil."* The governance of the internet, the regulation of data flows, and the assertion of digital sovereignty are now matters not just of commerce but of national security and geopolitical influence.

Who manages the internet's critical infrastructure? Where is user data stored, and under whose jurisdiction does it fall? Can India protect its citizens' digital rights while ensuring that its economy does not remain at the mercy of global technology giants? These questions lie at the heart of contemporary debates on internet governance and data sovereignty.

This chapter explores the institutional mechanisms that shape the global internet, India's evolving stance on sovereignty in cyberspace, the Draft Digital India Act of 2023, and the emerging paradigms of sovereign clouds and digital borders.

a. ICANN, ITU and the Global Norms Debate

Parameter	ICANN	ITU (International Telecommunication Union)
Nature	Multistakeholder, U.S.-origin non-profit	UN-based intergovernmental body
Role	Manages Domain Name Servers (DNS), allocates IP addresses	Coordinates global telecom standards and spectrum management
Criticism	U.S. dominance through historic oversight by its Department of Commerce	State-centric approach may restrict openness of the internet

- **ICANN (Internet Corporation for Assigned Names and Numbers):** Controls critical resources such as DNS and IP allocation. Long perceived as U.S.-centric, especially after the Snowden surveillance revelations.
- **China–Russia Bloc:** Advocates shifting authority to the UN-led ITU to reduce Western dominance.
- **India's Stand:** Initially leaned towards multilateralism (state-centric), but now supports a multistakeholder model—involving governments, civil society, and corporations—while proposing a UN Committee for Internet-Related Policies (CIRP) to balance inclusivity with legitimacy.

b. India's Push for Digital Sovereignty

India's assertive approach stems from the recognition that control over data is synonymous with control over power.

i. Why Digital Sovereignty Matters for India

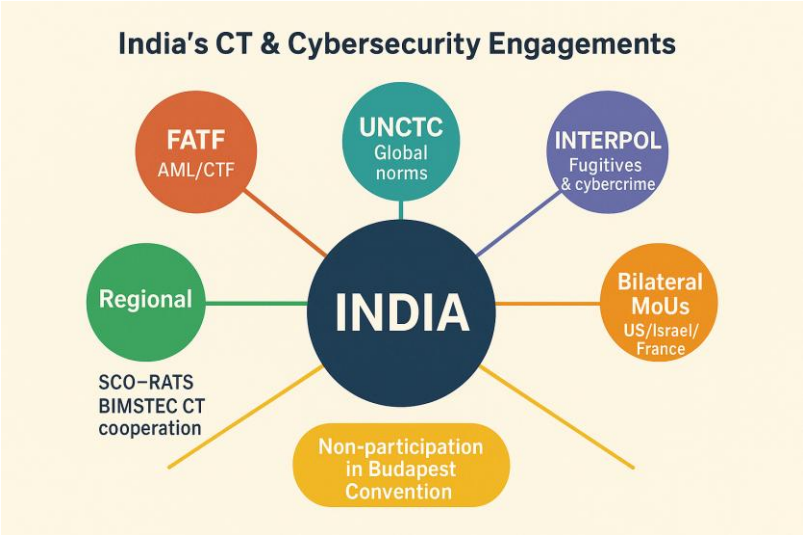
- **Security:** Overseas storage complicates law enforcement and delays investigations under MLATs.
- **Taxation:** Global tech firms extract value from Indian data without commensurate tax contributions.
- **Economic Growth:** Data localisation fuels domestic data centres, cloud providers, and AI startups.
- **Democratic Oversight:** Ensures Indian citizens' data is governed by Indian laws, not foreign jurisdictions.

ii. Benefits of Data Sovereignty

- Expansion of India's data centre industry, projected to be the world's second largest by 2050.
- Enhanced privacy and security under national jurisdiction.
- Aggregated data enabling AI-driven policymaking in areas like transport and health.
- Stronger investigative capacity for law enforcement agencies.

c. Draft Digital India Act (2023)

The Draft Digital India Act (2023) is India's most ambitious attempt to update digital regulation, replacing the outdated IT Act, 2000.



Key Provisions

- **User Rights Framework:** Stronger consent rules, grievance redressal, and parental controls.
- **Intermediary Regulation:** Strict due diligence on platforms like WhatsApp and Instagram.
- **Ban on Dark Patterns:** Prohibits manipulative interface designs.
- **Emerging Tech Coverage:** Extends accountability to AI, blockchain, and frontier technologies.
- **Children's Safety:** Introduces stringent safeguards against grooming and online exploitation.
- **Data Sovereignty Clause:** Mandates localisation of sensitive data within India.

The Act draws inspiration from the EU's GDPR and Digital Services Act, but adapts them to India's democratic and developmental context.

d. Sovereign Cloud and Digital Borders

- **Sovereign Cloud:**
  Infrastructure hosted and regulated within national borders, ensuring sensitive government and defence data remain under Indian jurisdiction.
  - *Example:* MeitY's Sovereign Cloud Platform for critical state functions.
  - *Benefits:* Military-grade security, financial transaction integrity, and AI-enabled e-governance.
- **Digital Borders:**
  Analogous to physical borders, maintained through:
  - National firewalls and routing controls.
  - Geo-fencing of sensitive data flows.
  - Surveillance mechanisms like NATGRID and the Centralised Monitoring System (CMS).
  - Mandatory localisation of specific categories of personal and strategic data.

Risks: Overregulation could stifle innovation, foster censorship, and isolate India from global data flows—undermining its ambitions to be a hub of the digital economy.

Conclusion

Internet governance and data sovereignty are now as central to national power as control over maritime routes was in the age of empires. For India, the challenge is to strike a balance between openness and autonomy—to assert digital sovereignty without sliding into protectionism or digital authoritarianism.

The path forward lies in:

- Strengthening India's role in global governance forums like ICANN and ITU.
- Enforcing selective localisation in sensitive sectors, while enabling cross-border digital trade.
- Building indigenous infrastructure—hyperscale data centres, sovereign AI models, secure cloud ecosystems.
- Championing equitable global cyber norms, positioning India as both a protector of citizens' rights and a driver of inclusive governance.

Ultimately, digital sovereignty is not merely about where data is stored, but about who sets the rules of the digital game.

"In the digital age, sovereignty is measured not in square miles, but in terabytes."

India's data centre industry is projected to become the world's second largest by 2050, highlighting the scale of opportunity tied to digital sovereignty.

The preceding chapters traced the architecture of India's security—from internal threats and maritime defence to cyberspace, space, and emerging technologies. Yet the true test of these frameworks lies in their application to live crises.

Contemporary events—whether a drone strike on a military base, a cyber breach of critical infrastructure, or maritime incursions in the Indian Ocean—reveal both the strengths and vulnerabilities of India's apparatus.

The next chapter therefore turns to Current Affairs, analysing recent developments, their security implications, and the lessons they hold for India's evolving strategy.

Chapter 19. Current Affairs

19.1 5G & Internal Security Implications

a. Introduction

5G (Fifth Generation Mobile Network) is not merely an incremental leap over 4G—it represents a transformative ecosystem. With speeds up to 100 times faster than 4G, ultra-low latency, and the capacity to connect billions of devices simultaneously, 5G underpins next-generation applications such as smart cities, autonomous vehicles, telemedicine, industrial automation, and AI-enabled governance.

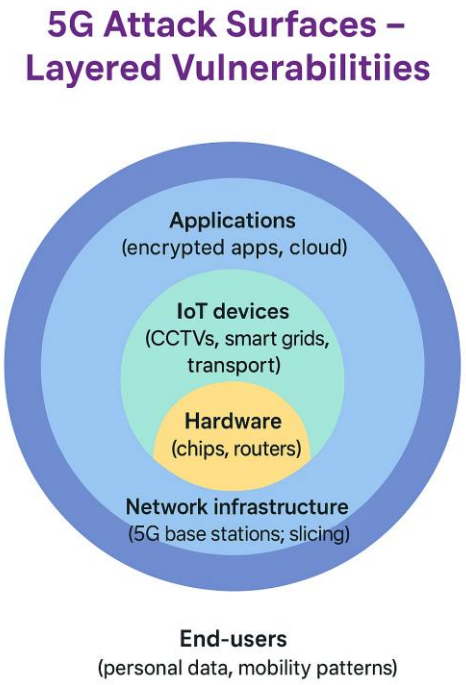
Yet, this unprecedented integration of digital networks with physical systems makes 5G a double-edged sword. On the one hand, it empowers policing, surveillance, and secure communication. On the other, it expands vulnerabilities—enlarging the attack surface, complicating lawful interception, and raising sovereignty concerns over foreign dependence. For India—already navigating hybrid warfare, narco-terrorism, and disinformation campaigns—the internal security implications of 5G are profound.

b. Security Opportunities from 5G

- **Enhanced Surveillance:** Real-time, high-definition streaming from CCTVs, drones, and bodycams; AI-driven crowd analysis.
- **Rapid Response:** Seamless coordination among police, CAPFs, and disaster-response units.
- **Smart Policing:** IoT-enabled predictive policing, geo-fencing, and facial recognition at scale.
- **Secure Communication:** Dedicated network "slices" for police, paramilitary, and defence, minimising interception risk.

c. Security Risks and Challenges

- **Expanded Attack Surface:** Billions of IoT devices—from traffic lights to hospital systems—can be hacked or manipulated.
- **Supply Chain Risks:** Dependence on foreign vendors (e.g., Huawei, ZTE) risks espionage via backdoors or malicious firmware.
- **Data Sovereignty Issues:** Enormous data flows without robust protection laws risk exploitation by hostile actors.
- **Encryption Challenges:** End-to-end encrypted 5G traffic complicates lawful interception for counter-terrorism.
- **Weaponisation of Autonomy:** Hijacked 5G-powered autonomous vehicles, drones, or robots could be used for terror strikes.



d. Implications for India's Internal Security

- **Counter-Terrorism:** Terror networks may exploit encrypted 5G apps for faster planning, shrinking detection windows.

- **Border Management:** 5G drones and sensors enable precision surveillance but remain vulnerable to jamming/spoofing.
- **Critical Infrastructure:** Smart grids, healthcare, and transport integrated with 5G face cyber-physical sabotage risks.
- **Law Enforcement:** Predictive policing can be revolutionised, but requires secure official 5G networks to avoid compromise.
- **Disinformation Warfare:** 5G amplifies deepfakes, propaganda, and communal disinformation at unprecedented speed.

e. Policy & Strategic Measures for India

- **Trusted Vendor Mandate:** Restrict 5G core networks to vetted suppliers via the "Trusted Telecom Portal."
- **5G Cybersecurity Framework:** Set IoT device standards, enforce network-slicing protections, and secure critical infrastructure.
- **Dedicated Security Slice:** Exclusive, encrypted 5G network for police, CAPFs, and emergency services.
- **Indigenous R&D Push:** Strengthen *Make in India* telecom manufacturing, chip design, and open-source 5G software stacks.
- **Inter-Agency Cyber Fusion:** Build 5G-specific threat cells across CERT-In, NCIIPC, and NTRO for rapid response.
- **Legal Readiness:** Update the IT Act and forthcoming Digital India Act to regulate 5G-enabled cybercrime and IoT misuse.

Conclusion

5G will be the nervous system of India's digital economy, governance, and security operations. While it promises efficiency and resilience, it also magnifies vulnerabilities across cyber, physical, and cognitive domains. India's path forward must be secure-by-design—embedding national security considerations at every layer of deployment, from hardware sourcing to data localisation and cyber resilience.

"With great connectivity comes great vulnerability. In the 5G era, security must travel at the speed of technology."

19.2 Cybersecurity – Risk Management Framework and Core Concepts

a. Introduction

In the digital age, cyberspace functions simultaneously as a decisive enabler and a latent Achilles' heel of national security. India's expansive digital ecosystem—spanning Aadhaar-linked governance platforms, the Unified Payments Interface (UPI), defence communication grids, and smart infrastructure—has vastly expanded the "attack surface" susceptible to exploitation.

A successful cyberattack no longer causes mere financial loss; it can paralyse power grids, disrupt healthcare delivery, compromise defence secrets, and erode citizen trust in the state.

To address these risks, two imperatives stand out:

- The adoption of a structured Risk Management Framework (RMF) that treats cybersecurity as a continuous cycle of identification, assessment, mitigation, response, and monitoring.

- A clear grounding in core cybersecurity principles, ensuring that defence measures remain both technically robust and strategically relevant.

b. Risk Management Framework (RMF)

The RMF is not a static compliance checklist but a dynamic, adaptive loop. Each stage feeds into the next, ensuring that systems evolve in tandem with adversary tactics.

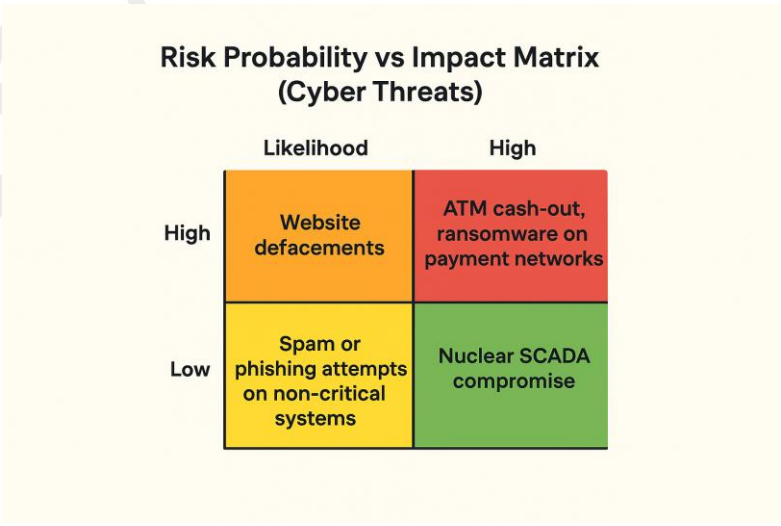
i. Risk Identification

The first task is to define what assets require protection and against whom.

- **Asset Mapping:** A full inventory of servers, endpoints, IoT devices, cloud environments, and proprietary software.
    - *Example:* In the banking sector, this includes core banking servers, SWIFT gateways, and ATM networks.
- **Threat Profiling:** Mapping adversaries based on intent and capability—from state-sponsored groups (e.g., APT41) to organised crime syndicates, hacktivists, and automated botnets.
- **Illustration:** In 2023, CERT-In alerts on UPI integration vulnerabilities enabled banks to isolate and patch high-risk systems before exploitation.

ii. Risk Assessment

Risks must then be prioritised by analysing likelihood and impact.



- **Likelihood:** Gauged from past incidents, active campaigns, and threat intelligence—often scored via the Common Vulnerability Scoring System (CVSS).
- **Impact:**
    - **High Impact:** Compromise of SCADA systems in nuclear plants.
    - **Medium Impact:** Defacement of a tourism website causing reputational harm but minimal disruption.
- **Illustration:** The RBI's cyber stress tests simulate ransomware attacks on payment gateways to measure systemic resilience.

iii. Mitigation and Controls

Controls are implemented across three dimensions:

- **Technical Controls:** Network segmentation, next-generation firewalls, intrusion detection, and strong encryption (e.g., AES-256 for data at rest; TLS 1.3 for data in transit).

- *Example:* In power plants, operational technology (OT) is air-gapped from IT systems to prevent lateral intrusion.

- **Administrative Controls:** Role-based access models, periodic security audits, and supply-chain vetting.
  - *Example:* MeitY mandates external audits for government platforms handling citizen data.
- **Physical Controls:** Restricted entry into server rooms, biometric access, CCTV monitoring, and electromagnetic shielding for sensitive defence equipment.

iv. Response and Recovery

Since no system is invulnerable, the aim is damage containment and swift restoration.

- **Incident Response Plans (IRP):** Define clear escalation paths, including forensic preservation of evidence.
- **Disaster Recovery Plans (DRP):** Ensure hot, warm, or cold backup sites with mirrored data centres across regions.
- **Illustration:** During the 2022 ransomware attack on AIIMS, manual record-keeping allowed continuity of patient care, while responders restored systems. This led to adoption of cloud-segmented backups.

v. Continuous Monitoring

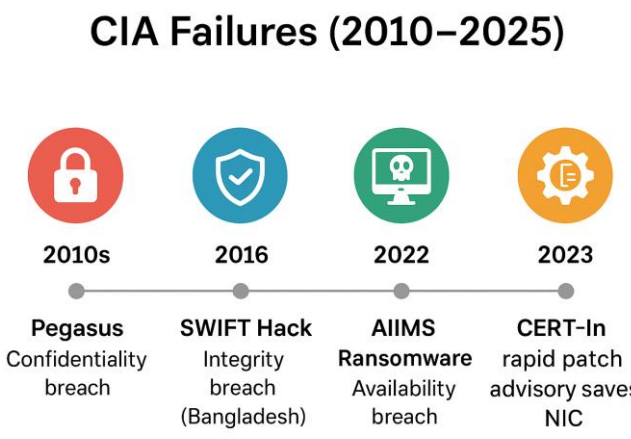
The final stage is real-time vigilance.

- **Security Operations Centres (SOC):** 24/7 monitoring of logs and anomalies using SIEM platforms like Splunk or IBM QRadar.
- **Threat Intelligence Feeds:** Early warnings from global cyber defence hubs anticipate new attack vectors.
- **Red-Teaming & Hunt Teams:** Proactively search for stealth intrusions.
- **Illustration:** The NCIIPC's surveillance of energy-sector SCADA systems has intercepted multiple intrusion attempts traced to foreign APTs.

The true power of the RMF lies in its adaptability. Each breach becomes a lesson learned, feeding back into the cycle to strengthen future defences. In doing so, resilience becomes embedded into the very architecture of the system.

c. Core Concepts of Cybersecurity

Cybersecurity rests on foundational concepts that guide both policy frameworks and technical safeguards. From the CIA Triad, which defines the objectives of protection, to the identification of attack surfaces and vectors, these principles form the backbone of all modern defence strategies.



i. The CIA Triad

At the heart of all cybersecurity doctrines lies the CIA Triad—Confidentiality, Integrity, and Availability. Referenced in frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and India's National Cyber Security Policy, the triad provides the gold standard for structuring security controls.

Confidentiality

Ensures that sensitive data is accessible only to authorised entities.

- **Mechanisms:** Strong encryption, secure protocols, access control systems, multi-factor authentication.
- **Illustration:**
    - Defence procurement plans are encrypted within the Ministry of Defence's secure network.
    - Aadhaar data is shielded through virtual IDs and biometric locking.
    - The Pegasus spyware controversy highlighted a breach of confidentiality through covert surveillance.

Integrity

Guarantees that data remains accurate and unaltered throughout its lifecycle.

- **Mechanisms:** Cryptographic hashing, digital signatures, immutable audit trails, version control systems.
- **Illustration:**
    - The GSTN tax database employs hashing to detect unauthorised changes.
    - Blockchain pilots in land registries provide tamper-proof records.
    - The 2016 SWIFT banking fraud in Bangladesh exposed the dangers of failing to safeguard transactional integrity.

Availability

Ensures that systems and information remain accessible whenever required.

- **Mechanisms:** Redundancy, load balancing, regular patching, and DDoS protection.
- **Illustration:**
    - The CoWIN vaccination platform scaled elastically to handle peak demand.
    - The RBI maintains disaster recovery sites for critical banking functions.
    - The AIIMS ransomware attack revealed the disruption caused when redundancy is absent.

ii. Attack Surfaces and Vectors

An attack surface is the total set of points where an adversary might attempt to gain entry or extract sensitive information. Attack vectors are the specific methods used to exploit these points. Together, they define the avenues of risk in cyberspace.

For clarity, risks can be examined across four interlinked layers:

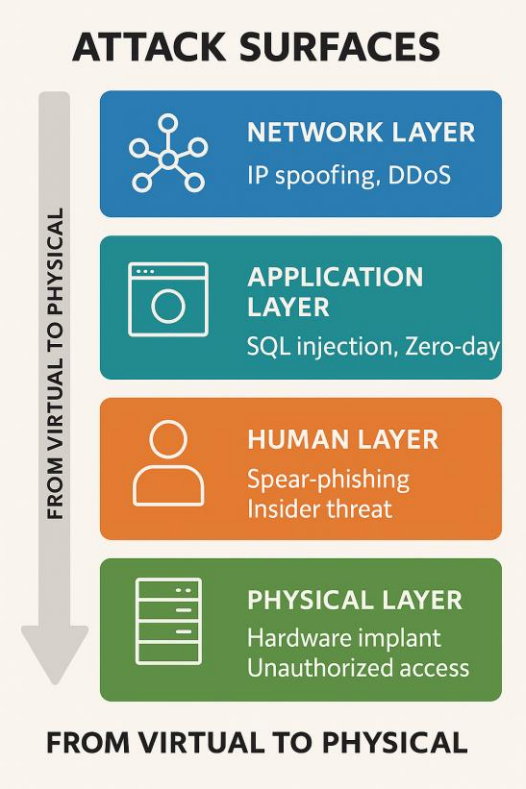
Network Layer

The foundational layer, vulnerable to deceptive or overwhelming techniques.

- **IP Spoofing:** Attackers forge source addresses to impersonate trusted systems and bypass controls.
    - *Example:* During political unrest, spoofed "government IPs" have been used to evade firewalls.

- *Defence:* Strict firewall access lists, reverse path forwarding, cryptographic authentication.

- **DDoS Attacks:** Servers are overwhelmed with traffic, disrupting services.
  - *Example:* Jammu and Kashmir administration portals were targeted during unrest.
  - *Defence:* Load balancing, content distribution networks, ISP-level filtering, scrubbing centres.



Application Layer

Targets software and platforms that directly interface with users.

- **SQL Injection:** Malicious queries manipulate backend databases.
  - *Example:* Attempts made to breach Aadhaar-linked repositories.
  - *Defence:* Parameterised queries, server-side validation, Web Application Firewalls.

- **Zero-Day Exploits:** Vulnerabilities unknown to vendors exploited for admin-level access.
  - *Example:* Indian e-governance portals probed using such flaws.
  - *Defence:* Timely patching, sandbox testing, proactive intrusion detection.

Human Layer

The weakest link, where adversaries exploit human fallibility.

- **Spear-Phishing:** Personalised emails deceive officials into sharing credentials or downloading malware.
  - *Example:* Groups like SideWinder have targeted Indian defence personnel via fake seminar invites.
  - *Defence:* Awareness training, phishing-resistant MFA, advanced email scanning.

Physical Layer

The hardware dimension, where compromise occurs at the component level.

- **Hardware Implants:** Malicious chips or modified parts inserted into imported telecom/IT equipment.
  - *Example:* Concerns over unvetted foreign telecom gear.
  - *Defence:* Vendor vetting, tamper-proof packaging, independent audits, supply-chain security protocols.

A holistic understanding of attack surfaces and vectors underpins India's National Cyber Security Strategy, which stresses multi-layered defences across civilian, commercial, and defence networks.

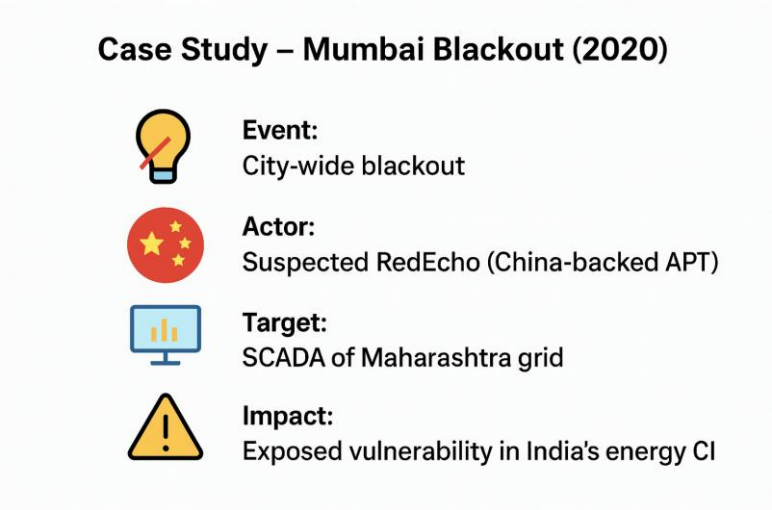
iii. Critical Infrastructure Protection (CIP)

Definition and Significance

Critical Infrastructure (CI) refers to assets, systems, and networks—both physical and digital—whose disruption would severely impair national security, economic activity, public health, or societal stability. In today's interconnected era, this extends beyond power plants and transport hubs to include Supervisory Control and Data Acquisition (SCADA) systems, Industrial Control Systems (ICS), and cloud-hosted command networks.

For India, protecting CI is an existential priority. The adoption of smart grids, digital payments, e-governance, and space-based navigation has multiplied dependence on such systems, while simultaneously widening their vulnerability.

Sectors at Risk



- **Energy:** Power grids, oil pipelines, and nuclear plants are exposed to blackouts and cascading safety failures.
- **Banking and Finance:** RBI payment systems, stock exchanges, and UPI gateways are lucrative targets for cyber theft and disruption.
- **Telecommunications:** Mobile networks, submarine cables, and internet exchange points can act as choke points; their disruption could isolate entire regions or the nation.
- **Defence Manufacturing:** Laboratories and ordnance factories face risks of intellectual property theft and sabotage.
- **Space Assets:** Navigation satellites and data centres risk GPS spoofing or hijacking.

Indian Mechanisms for CIP

- **NCIIPC (National Critical Information Infrastructure Protection Centre):** Established under Section 70 of the IT Act (2000); identifies critical sectors, conducts audits, issues advisories, and coordinates with sectoral CERTs.
- **CERT-In (Indian Computer Emergency Response Team):** The national nodal agency for vulnerability monitoring, alerts, and incident coordination.
- **Cyber Swachhta Kendra:** Offers free tools for malware and botnet removal, indirectly securing public and private networks that underpin CI.
- **Sectoral Regulations:** RBI's cyber framework for banks, CERC's cybersecurity guidelines for power grids, and DoT's directives for telecom operators.

Case Study: 2020 Mumbai Power Outage

In October 2020, a massive blackout paralysed Mumbai, impacting hospitals, stock exchanges, and rail services. Cyber intelligence firms linked the breach to RedEcho, a suspected China-backed APT group, which allegedly infiltrated SCADA systems of the Maharashtra State Electricity Board. While no official attribution was confirmed, the incident underscored both the fragility of energy infrastructure and the strategic messaging potential of cyberattacks on civilian systems.

iv. Cyber Hygiene and Organisational Practices

If CI is the body of the digital nation, then cyber hygiene is its daily discipline. These practices are simple but indispensable, reducing vulnerabilities by embedding vigilance into organisational culture.

Patch Management

- **Risk:** Unpatched systems remain the most common breach vector; ransomware like WannaCry exploited outdated Windows flaws.
- **Practice:** Automated patch schedules with critical fixes applied within 24–72 hours.
- **Example:** Despite CERT-In advisories, lapses have caused government portal leaks.

Multi-Factor Authentication (MFA)

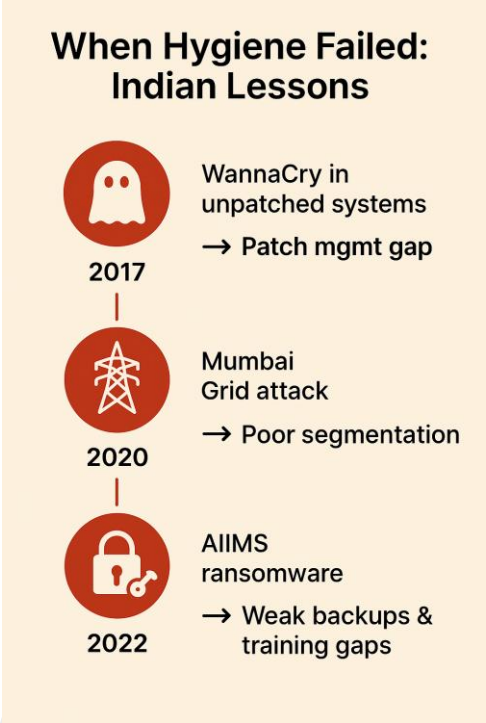
- **Risk:** Passwords alone are inadequate.
- **Practice:** MFA combines knowledge (password), possession (token), and inherence (biometric).
- **Example:** FIDO2 keys for defence email accounts now protect against account takeovers.

Network Segmentation

- **Risk:** Flat networks allow attackers lateral movement.
- **Practice:** Use of VLANs, firewalls, and jump hosts to isolate critical systems.
- **Example:** In the 2020 Mumbai grid breach, stronger segmentation could have prevented cross-movement between corporate IT and operational SCADA.

Backup Protocols

- **Risk:** Ransomware cripples live data, paralysing systems.
- **Practice:** Apply the 3-2-1 rule—three copies, two storage media, one offline/offsite.
- **Example:** The RBI mandates offline backups for Core Banking Systems, ensuring financial resilience.



Awareness Training

- **Risk:** Humans remain the weakest link, vulnerable to phishing and social engineering.
- **Practice:** Quarterly phishing simulations, role-based training, and awareness campaigns.
- **Example:** NCIIPC advocates mandatory phishing drills across all CI operators.

Conclusion

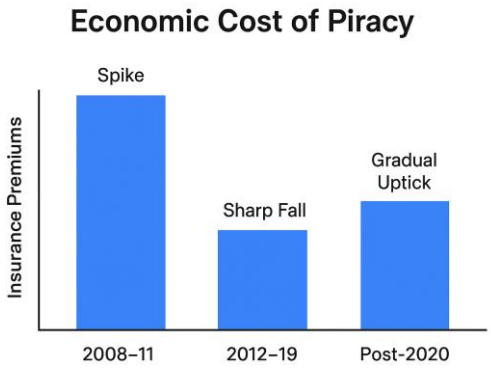
The interplay of attack surfaces, critical infrastructure, and cyber hygiene reveals a central lesson: cybersecurity is not won through technology alone but through disciplined processes, layered defences, and cultural habits of vigilance. India's digital resilience depends as much on patching on time, backing up data, and questioning suspicious emails as on deploying advanced firewalls or satellites.

As one expert observes: *"Cybersecurity is not a product you buy; it is a practice you cultivate."*

19.3 Piracy in the Indian Ocean

a. Introduction

The Indian Ocean Region (IOR)—the world's third-largest maritime expanse—is a critical artery of global trade. Nearly half of global container traffic, 40% of oil shipments, and over two-thirds of petroleum products transit through its waters. Within this theatre, piracy has emerged as a recurring threat—particularly in the Gulf of Aden, Somali Basin, Arabian Sea, and Northern Mozambique Channel—jeopardising Sea Lines of Communication (SLOCs) vital to India's economy and global trade.



While multinational naval operations and onboard security measures drastically curtailed piracy after its 2011 peak, recent years have seen signs of resurgence. Political instability, economic distress in littoral states, reduced foreign naval presence, and the convergence of piracy with other maritime crimes are reviving concerns that piracy could once again destabilise one of the world's busiest sea lanes.

b. Historical Context

- **2005–2011: Somali Piracy Peak**
  Explosive surge in piracy targeted oil tankers, container vessels, and trawlers. Ransoms for hijacked ships exceeded USD 5 million, with over 200 attacks in 2011 alone.
- **2012–2019: Decline**
  Coordinated naval patrols—EUNAVFOR, NATO operations, Combined Maritime Forces (CMF)—and armed guards onboard vessels sharply reduced incidents.
- **Post-2020: Renewed Concerns**
  COVID-19 economic shocks, fragile governance in Somalia and Yemen, and scaled-down international naval presence created space for revival.

c. Geographic Hotspots

Area	Piracy Characteristics	Strategic Significance
Gulf of Aden	Skiff attacks on slow-moving vessels amid dense traffic	Chokepoint linking Europe and Asia
Somali Basin	Long-range raids using mother ships	Deep-sea access to East African routes
Arabian Sea	Intermittent piracy, often tied to narcotics	Direct approach to India's west coast
Mozambique Channel	Armed robbery and piracy linked to insurgencies	Key trade corridor with Southern Africa

d. Causes of Piracy in the IOR

- Weak governance and fragile law enforcement in littoral states.
- Economic deprivation and unemployment in coastal communities.
- IUU fishing by foreign fleets, fuelling resentment among locals.
- Convergence with smuggling networks—arms, narcotics, and human trafficking.
- Dense maritime traffic, offering lucrative and accessible targets.

e. Tactics and Trends

- **Mother Ship Operations:** Larger vessels extend reach and complicate detection.
- **Kidnap-for-Ransom:** Crew abductions more common than full ship seizures.
- **Disguised Fishing Vessels:** Pirates blend with legitimate traffic.
- **Technology Use:** GPS and satellite links enable targeted precision strikes.

f. India's Response and Role

- **Naval Deployments:** Since 2008, the Indian Navy has maintained continuous anti-piracy patrols in the Gulf of Aden, extended under Mission-Based Deployments to East Africa and wider IOR.
- **Convoy System:** Escorts for Indian-flagged and high-risk vessels.
- **Operational Successes:** Regular interceptions of pirate dhows and rescues, including the 2024 liberation of MV Lila Norfolk from hijackers in the Arabian Sea.
- **Information Sharing:** IFC-IOR (Information Fusion Centre–Indian Ocean Region) in Gurugram strengthens intelligence coordination.
- **Capacity Building:** Joint patrols, training, and equipment support to littoral states—Oman, Seychelles, Mauritius, Madagascar.

g. Challenges

- Vast IOR expanse makes continuous coverage resource-intensive.
- Jurisdictional gaps and uneven national piracy laws complicate prosecution.
- Pirates adapt with hybrid tactics, merging piracy with smuggling or terror.
- Use of private armed guards raises liability and risk of escalation.

h. Implications for Internal and Maritime Security

- **Energy Security:** Threatens India's oil and gas imports.
- **Human Security:** Endangers Indian seafarers, who form a major share of the global merchant navy.
- **Economic Costs:** Raises insurance premiums, reducing competitiveness of Indian trade.
- **Terror Linkages:** Ransom money and smuggling routes may feed extremist networks.

Conclusion

Piracy in the IOR is both a law-and-order problem and a strategic challenge. For India, securing SLOCs is essential not only for trade and energy but also for its role as a net security provider in the region. The way forward lies in sustained naval vigilance, robust international cooperation, and socio-economic stabilisation of piracy-prone littorals. Without this, the spectre of the early 2010s could return, undermining regional maritime stability.

"Piracy thrives where governance sinks—security at sea begins with stability on shore."

Indian seafarers constitute nearly 10% of the global merchant navy workforce, making piracy not just a trade risk but also a direct human security concern for India.

19.4 Immigration, Refugees and India's Security

a. Introduction

Immigration refers to the movement of foreign nationals into a country for residence, work, or other purposes. Refugees, by contrast, are individuals compelled to leave their home state due to persecution, conflict, or disaster, seeking protection elsewhere.

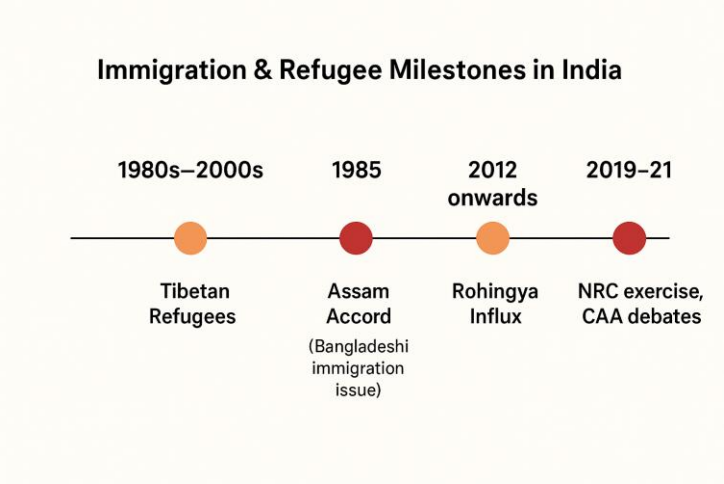
For India, regulated immigration contributes positively by enriching the economy and society. Yet illegal immigration and uncontrolled refugee influx generate profound internal security challenges: demographic transformation in sensitive regions, exploitation of refugee communities by extremist groups, and diplomatic friction with neighbours.

As former National Security Adviser Shivshankar Menon observed, borders are not merely lines of control but "lines of trust and resilience." This is nowhere truer than in the management of cross-border human flows.

b. Categories of Concern

i. Illegal Immigrants

- Persistent challenge of Bangladeshi nationals entering Assam, Tripura, and West Bengal without documentation.
- Settlement alters ethnic balances, fuels tensions, and strains scarce resources.



ii. Refugees (Recognised and Unrecognised)

- India has hosted Rohingya Muslims from Myanmar, Sri Lankan Tamils during the civil war, and Afghan refugees.
- Reflects India's humanitarian ethos, but such groups remain vulnerable to extremist exploitation and generate local friction.

iii. Asylum Seekers

- Tibetans (since 1959) and political dissidents from neighbouring states found asylum in India.
- While showcasing moral leadership, such decisions carry sensitive geopolitical consequences, straining ties with origin countries.

c. Key Security Concerns

- **Demographic Change:** Large-scale immigration has altered ethnic compositions in Assam and Tripura, sparking the Assam Agitation and NRC exercises.
- **Extremism Risks:** Refugee camps are vulnerable to radicalisation; Rohingya settlements have drawn repeated security scrutiny.
- **Border Strain:** Porous frontiers with Bangladesh, Myanmar, and Nepal enable unchecked crossings and facilitate arms/narcotics trafficking.
- **Resource Pressure:** Sudden influx overwhelms housing, healthcare, and education, generating resentment.
- **Organised Crime:** Smuggling, trafficking, and document forgery networks thrive in migration corridors.

d. Case Examples

- **Bangladeshi Immigration:** Persistent demographic and political tensions in Assam, Tripura, and West Bengal, culminating in the Assam Accord (1985) and NRC debates.
- **Rohingya Influx (post-2012):** Settled in Jammu, Delhi, Hyderabad; flagged in intelligence reports for extremist linkages.
- **Sri Lankan Tamil Refugees (1980s–2000s):** While mostly victims of war, LTTE cadres exploited camps for logistics and recruitment.
- **Tibetan Refugees (since 1959):** Politically sensitive, straining India–China relations, with settlements in Himachal Pradesh, Karnataka, Arunachal Pradesh.

e. Legal and Policy Framework

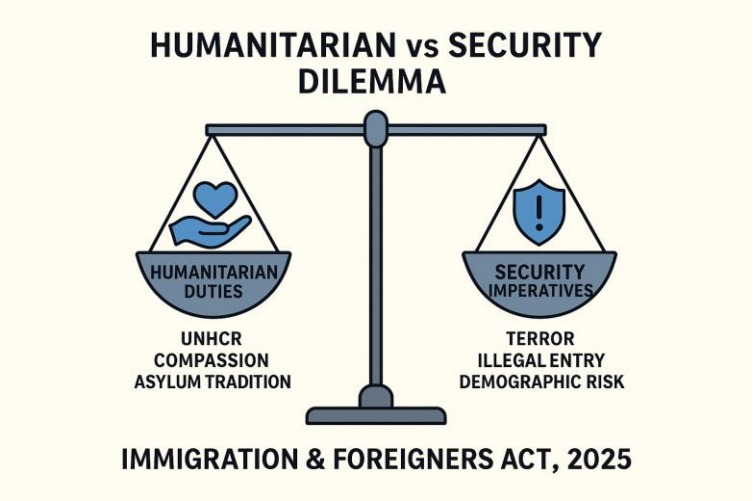
India is not a signatory to the 1951 Refugee Convention or its 1967 Protocol, managing refugees on a case-by-case basis. Cooperation with UNHCR supplements this framework.

Evolution of Legal Instruments

Pre-2025 Law	Year	Key Features	Replaced by
Foreigners Act	1946	Defined "foreigner"; empowered detention/deportation	Immigration and Foreigners Act, 2025
Registration of Foreigners Act	1939	Mandatory FRRO registration	Immigration and Foreigners Act, 2025
Passport (Entry into India) Act	1920	Required valid passport for entry	Immigration and Foreigners Act, 2025
Immigration (Carrier's Liability) Act	2000	Carriers liable for undocumented passengers	Immigration and Foreigners Act, 2025

Immigration and Foreigners Act, 2025

A consolidated statute modernising India's immigration law. Key features:



- National Immigration Authority under MHA to unify passports, visas, registration, deportation.
- Mandatory registration for long-term visitors; penalties for violations.
- Carrier liability with advance passenger data requirements.
- Stringent penalties for illegal entry or forged documents (up to 3 years imprisonment and ₹5 lakh fine).
- Digital vetting: biometric platforms and district-level monitoring.

This reform streamlines outdated laws and aligns India with hybrid-era threats like forged identities and cyber-enabled fraud.

f. Measures Taken

- **Border Infrastructure:** Fencing, floodlighting, and Integrated Check Posts on sensitive frontiers.
- **Smart Surveillance:** Drones, thermal imagers, and BOLD–QIT smart fencing projects.
- **Deportation/Repatriation:** Illegal immigrants identified and returned via diplomatic channels.
- **Screening/Vetting:** Monitoring of refugee camps for extremist activity.
- **Legal Action:** Crackdowns on forged documents, trafficking, and immigration rackets.

g. Challenges

- **No Dedicated Refugee Law:** Ad hoc approach creates inconsistency.
- **Humanitarian vs Security Dilemma:** Balancing compassion with vigilance.
- **Political Sensitivity:** Immigration is deeply tied to electoral politics, especially in the Northeast.
- **Verification Gaps:** Many immigrants lack authentic documents, enabling identity fraud.
- **Regional Instability:** Crises in Myanmar, Afghanistan, Bangladesh risk sudden influxes.

Conclusion

Immigration and refugee flows are double-edged: enriching when managed transparently but destabilising when uncontrolled. India's imperative is to blend robust border management, transparent refugee policies, and community integration—ensuring vulnerable groups are not alienated, while hostile actors are denied exploitation.

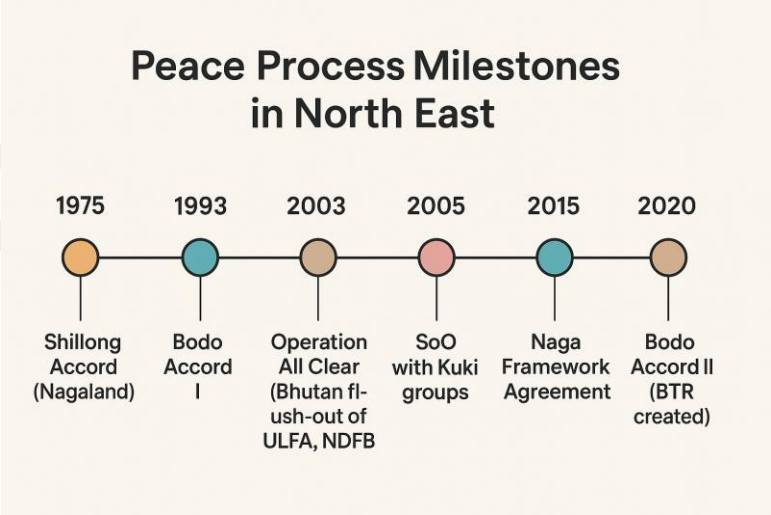
"Security without compassion is inhuman; compassion without security is naïve."

India currently hosts over 200,000 refugees and asylum seekers from more than 20 countries, despite lacking a dedicated refugee law.

19.5 North East Insurgency

a. Introduction

The insurgency landscape of India's Northeast is among the most complex in the world. Unlike a unified rebellion, it is marked by multiple ethnic-based armed groups, each pursuing distinct and often conflicting objectives.



Factionalism is the defining feature—driven by tribal rivalries, overlapping territorial claims, ideological disagreements, and frequent splintering during peace processes. This fragmentation has created an unstable security environment where no single settlement framework can accommodate the diversity of grievances.

Thus, insurgency in the Northeast is not merely a law-and-order issue, but a deeply political and societal challenge.

b. Major Insurgent Groups and Core Demands

State / Region	Major Factions	Core Demands	Notes
Nagaland	NSCN (Isak-Muivah), NSCN (Khaplang–YA), NSCN (Reformation)	"Greater Nagalim" integrating Naga-inhabited areas across	NSCN (IM) signed 2015 Framework Agreement; final settlement elusive;

State / Region	Major Factions	Core Demands	Notes
		Northeast & Myanmar, with special constitutional status	neighbouring states oppose redrawing boundaries
Manipur – Kuki Groups	Kuki National Organisation (KNO), United People's Front (UPF)	Kukiland Territorial Council / autonomy under Sixth Schedule provisions	Under Suspension of Operations; overlaps with Naga claims
Assam – Bodo Groups	NDFB factions, ABSU	Separate Bodoland state / enhanced territorial autonomy	2020 Bodo Accord created Bodoland Territorial Region, but splinter factions remain restless
Assam – ULFA	ULFA (Independent – Paresh Baruah), ULFA (Pro-Talks)	Sovereign Assam (ULFA-I); autonomy and identity safeguards (ULFA-PT)	Talks ongoing with ULFA-PT; ULFA-I operates from Myanmar bases
Tripura	NLFT, remnants of ATTF	Independent Tripura, expulsion of non-tribals	Weakened since 2005; small cells survive
Meghalaya	HNLC, remnants of GNLA	Greater autonomy for Khasi-Jaintia & Garo Hills	GNLA neutralised; HNLC exploring talks
Arunachal Pradesh	ENNG and smaller Naga groups	Autonomy for Eastern Nagaland areas	Linked to Naga insurgency dynamics

c. Key Issues Arising from Factionalism

- **Overlapping Territorial Claims:** Contest between Nagas and Kukis in Manipur hills, or Bodos and other tribes in Assam, often leads to violence.
- **Splintering During Peace Talks:** Negotiations trigger splits into pro-talks and hardline factions, ensuring conflict persists.
- **Parallel Governance Structures:** Insurgent groups run shadow administrations—collecting taxes, enforcing laws—undermining state legitimacy.
- **Ceasefire Contradictions:** Different Suspension of Operations (SoO) terms create loopholes, exploited by cadres moving across states.
- **Cross-Border Sanctuaries:** Safe havens in Myanmar, Bangladesh, and Bhutan provide training, regrouping, and arms smuggling routes.
- **Ethnic Polarisation:** Identity-driven narratives deepen divides, making reconciliation difficult.

d. Internal Security Implications

- **Prolonged Low-Intensity Conflict:** Persistent violence drains resources and stalls development.
- **Fragile Ceasefires:** Ethnic clashes erupt even during truce periods, reflecting instability.
- **Border Pressures:** Cross-border sanctuaries add strain to border management forces.
- **Fragmented Negotiations:** Government is forced into parallel, inconsistent dialogues, diluting coherence.

e. Policy Considerations

- **Integrated Peace Framework:** A multi-party platform to address overlapping claims and avoid piecemeal settlements.
- **Harmonised Ceasefire Monitoring:** Standardised mechanisms across agreements to close loopholes.
- **Confidence Building Between Ethnic Groups:** Promote inter-tribal governance and development initiatives to weaken polarisation.
- **Cross-Border Cooperation:** Stronger security ties with Myanmar and Bangladesh to dismantle sanctuaries.
- **Phased Demobilisation and Rehabilitation:** Clear, uniform reintegration guidelines to prevent relapse into militancy.

Conclusion

Factionalism is the greatest obstacle to peace in the Northeast. Divergent demands, overlapping territorial ambitions, and entrenched ethnic divisions ensure that partial settlements leave dissatisfied factions to continue militancy.

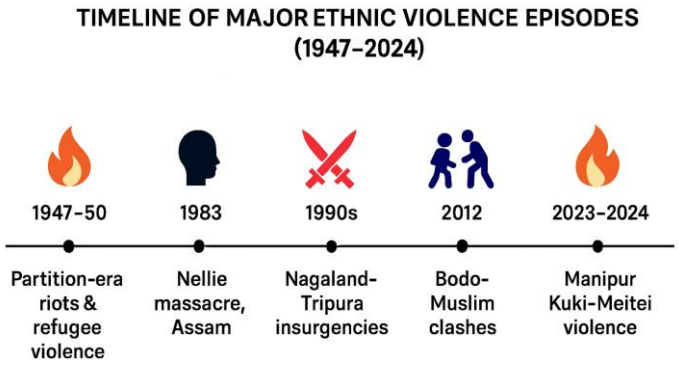
Sustainable peace requires an inclusive, consensus-driven framework that addresses security, identity, and development together.

"In the North East, peace cannot be made in fragments—it must be woven together."

As of 2024, over 60 insurgent groups in the Northeast have signed Suspension of Operations or peace agreements, yet splinter factions continue to sustain violence.

19.6 Ethnic Violence

a. Introduction



Ethnic violence refers to conflict between communities distinguished by identity—whether tribe, language, religion, or ethnicity—where identity itself becomes the rallying point for hostility. In India, such violence emerges when historical grievances, uneven development, demographic shifts, and political mobilisation of identity converge.

The recent Manipur crisis (2023–24), marked by Kuki–Meitei tensions, brought ethnic conflict back to the centre of national discourse. Earlier episodes, such as the Bodo–Muslim clashes in Assam (2012) and tensions linked to Rohingya refugees in the Northeast, underline that such violence is no longer confined to remote tribal belts—it can erupt suddenly, spill across borders, and destabilise entire regions.

From an internal security perspective, ethnic violence is more than a humanitarian tragedy. It erodes state authority, creates governance vacuums, and provides fertile ground for insurgent, extremist, and external actors. Most importantly, its persistence challenges the pluralist ideals of the Indian Constitution, particularly Article 14 (equality before law) and Article 21 (life and liberty).

b. Causes of Ethnic Violence

Ethnic violence rarely has a single trigger. It typically arises from a web of reinforcing factors:

- **Historical Grievances:** Colonial-era divisions, Partition-era displacements, and tribal alienation resurface during political or economic stress. The legacy of land alienation in the Northeast remains a persistent fault line.
- **Uneven Development:** Disparities in infrastructure, education, and jobs deepen insecurities. The hills–valley divide in Manipur or Bodo–non-Bodo economic competition in Assam exemplify how uneven growth hardens identity politics.
- **Identity Politics:** Electoral mobilisation on ethnic lines entrenches fault lines. Ethnic-based parties in the Northeast often shape governance in exclusionary ways.
- **Demographic Change:** Migration—internal or cross-border—triggers fears of marginalisation. Illegal immigration in Assam and Rohingya influxes in border states sharpen insecurities.
- **Resource Competition:** Scarce land, forests, jobs, and political representation are perceived as zero-sum contests. The Meitei demand for ST status, opposed by Kukis, reflects such anxieties.
- **External Influence:** Cross-border kinship enables external states and non-state actors to provide funding, arms, or ideological support. Myanmar-based insurgent sanctuaries, for instance, have been linked to tribal militias in Manipur and Nagaland.

c. Consequences of Ethnic Violence

The impact of ethnic violence is multidimensional, producing spirals that are hard to break:

- **Humanitarian:** Mass displacement, refugee flows, and loss of lives. The 2023 Manipur violence displaced over 60,000 people, echoing earlier Assam clashes.
- **Economic:** Local economies collapse, investment stalls, and development projects are abandoned. Prolonged internet shutdowns in Manipur in 2023 dented its GDP measurably.
- **Social Fragmentation:** Parallel governance emerges, communities ghettoise, and trust collapses. Armed "village defence committees" often supplant the state.
- **Cycles of Revenge:** Retaliatory killings and reprisals sustain conflict, as seen in Nagaland during the 1990s.
- **Security Vacuum:** Militias and insurgents thrive in governance gaps. The rise of "armed volunteers" in Manipur illustrates this erosion of state credibility.
- **Governance Strain:** Extraordinary measures such as AFSPA are reimposed, diverting focus to policing rather than long-term reconciliation.

d. Mitigation Strategies

Managing ethnic violence requires an integrated approach of security, governance, and reconciliation:

- **Constitutional Safeguards:** Strengthen Sixth Schedule provisions, PESA Act protections, and customary law frameworks, while ensuring they do not fragment national unity.
- **Institutional Mechanisms:** Establish district- and state-level inter-community councils for structured dialogue and rapid grievance redressal.
- **Inclusive Development:** Deliver targeted packages for marginalised groups, ensure equitable land/job distribution, and guarantee transparent welfare delivery.
- **Cultural Diplomacy:** Promote inter-ethnic exchanges, shared sports, and heritage projects that foster common identities beyond narrow ethnic lines.
- **Security–Governance Balance:** Deploy security forces to restore order, but pair with phased withdrawal of extraordinary powers, truth-telling, and justice mechanisms.
- **Digital Regulation:** Invest in fact-checking, cyber monitoring, and counter-deepfake units to prevent online hate campaigns from triggering unrest.

Conclusion

Ethnic violence is not merely a breakdown of law and order—it is a rupture in the social fabric, where identity becomes the instrument of exclusion and hostility. While security forces may restore temporary calm, enduring peace demands structural reforms: inclusive governance, equitable development, and sustained dialogue.

For India, the imperative is to transform ethnic diversity from a fault line into a shared strength, aligning constitutional values with recognition of each community's unique cultural and historical identity. In an era where local tensions can swiftly spill across borders, proactive prevention and reconciliation are not optional—they are essential.

As a senior peace negotiator observed: *"Ethnic peace cannot be imposed—it must be patiently built, until diversity becomes strength, not fear."*

19.7 China-Specific Threats

a. Introduction

China today represents India's most formidable strategic competitor. With the world's second-largest defence budget, rapidly modernising armed forces, and expanding capabilities in space, cyber, and artificial intelligence, Beijing has the ability to project power across multiple domains.

Its military–industrial ecosystem thrives on a blend of state-driven technology acquisition, aggressive reverse engineering, cyber-enabled espionage, and indigenous research, giving China a decisive edge in creating platforms that integrate land, sea, air, space, and cyberspace operations into a seamless whole.

For India—sharing a long, contested boundary with China while competing in the Indian Ocean and emerging technologies—the threat is neither abstract nor distant. It is an evolving challenge that combines conventional military pressure with hybrid and grey-zone tactics.

b. Defence Budget Comparison

China's defence expenditure (2024): ~USD 224–230 billion (second only to the US).
India's defence expenditure (2024): ~USD 73–75 billion (third globally, but less than one-third of China's).

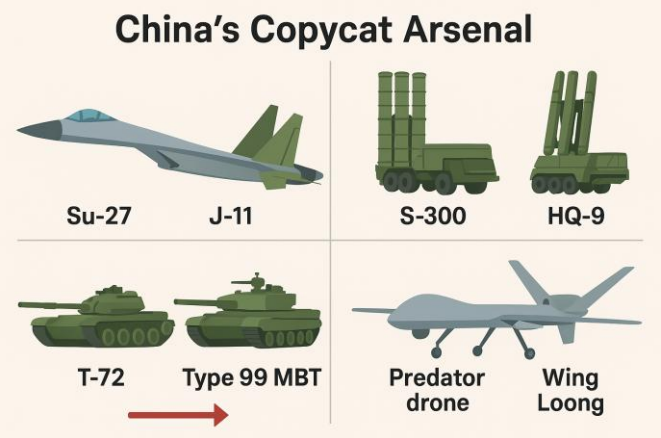
Implications of this disparity:

- Beijing can sustain longer, multi-theatre operations with superior funding.
- It inducts next-generation systems—fifth-generation fighters, aircraft carriers, hypersonic missiles—at a faster pace.
- Continuous R&D investment gives China a structural innovation advantage.

c. Reverse Engineering

A hallmark of China's modernisation has been the rapid indigenisation of foreign technology.

- **J-11 Fighter:** Reverse engineered from Russia's Su-27.
- **HQ-9 Missile System:** Derived from Russia's S-300.
- **Type-99 Main Battle Tank:** Incorporates adaptations from multiple foreign designs.



Risks for India:

- China's reduced dependence on external suppliers for critical platforms.
- Mass production at lower cost, giving the PLA numerical superiority, especially along the LAC.

d. Technology Theft

Beyond reverse engineering, China aggressively pursues cyber espionage, insider recruitment, and academic partnerships.

- **Hacker groups (APT10, APT41):** Target defence contractors, aerospace firms, and strategic industries worldwide.
- **Thousand Talents Plan:** Recruitment drive incentivising scientists to transfer sensitive IP.

Implications for India:

- Strategic agencies such as DRDO, ISRO, and DPSUs face constant targeting.
- Successful penetrations could erode India's edge in space, missile systems, and AI technologies.

e. Anti-Satellite (ASAT) Weapons

- **2007:** China demonstrated ASAT capability by destroying one of its own satellites (865 km altitude), creating large-scale orbital debris.
- **Current Arsenal:** Believed to include direct-ascent missiles, co-orbital "killer satellites," and electronic/laser-based jammers.

Strategic Objective: Deny adversaries access to C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance) systems during conflict.

Implications for India:

- Threat to satellites critical for NavIC navigation, secure communication, and military surveillance.
- A targeted strike could cripple command-and-control structures during high-intensity conflict.

f. Multi-Domain Threat Synthesis

China's military posture extends across all operational domains, making it a systemic rather than a limited challenge.

- **Land Warfare:** A modernised ground force, supported by extensive LAC infrastructure, enables rapid mobilisation in disputed Himalayan sectors.
- **Naval Power:** The PLAN (People's Liberation Army Navy) is evolving into a true blue-water force, deploying aircraft carriers and nuclear submarines capable of threatening India's Sea Lines of Communication (SLOCs) in the Indian Ocean.

- **Air Power:** Fifth-generation fighters such as the J-20 and long-range bombers give Beijing the capacity to establish air superiority in regional theatres.
- **Cyber Domain:** State-backed hacker units hold the ability to disrupt Indian critical infrastructure, financial systems, and defence networks.
- **Space Domain:** With its expanding ASAT arsenal and space-based ISR, China can degrade or deny India's orbital assets in wartime.

Synthesis: China cannot be seen merely as a conventional adversary on the Himalayan frontier. It must be understood as a systemic competitor across the full spectrum of national power—military, technological, and economic.

g. India's Counter-Measures

India has initiated a multi-pronged response, blending capability development, institutional reform, and strategic partnerships:

- **Capability Development:** Induction of Tejas Mk-2, the Advanced Medium Combat Aircraft (AMCA), and Arihant-class nuclear submarines to strengthen indigenous power projection.
- **Space Security:** Expansion of the Defence Space Agency, focus on satellite redundancy, and hardening of orbital assets against hostile action.
- **Cyber Defence:** Strengthening of the Defence Cyber Agency and CERT-In to secure networks and protect research ecosystems.
- **Technology Protection:** Rigorous procurement vetting and tighter academic–industry controls on sensitive projects to limit espionage risks.
- **Diplomatic Engagement:** Building coalitions such as the Quad and deepening partnerships in the Indian Ocean Region (IOR) to counterbalance China's maritime expansion.

Conclusion

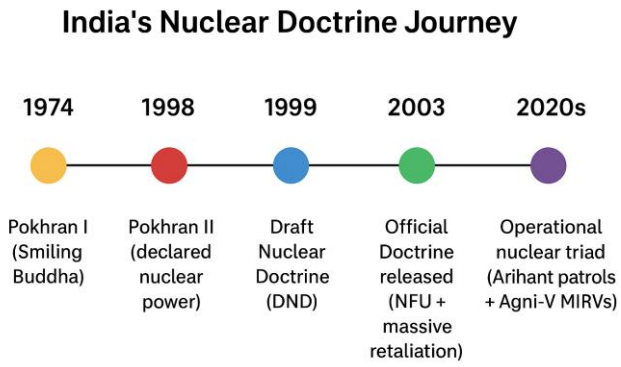
China's sustained defence spending, aggressive technology acquisition, and expanding cyber–space capabilities present India with a multidimensional challenge. The asymmetry is not merely in scale but also in quality, reflected in Beijing's ability to integrate military, technological, and economic tools into a single, coordinated strategy of power projection.

India's response must be equally comprehensive—focusing on military modernisation, ecosystem protection, cyber and space resilience, and deeper partnerships with like-minded states.

19.8 India's Nuclear Doctrine

a. Introduction

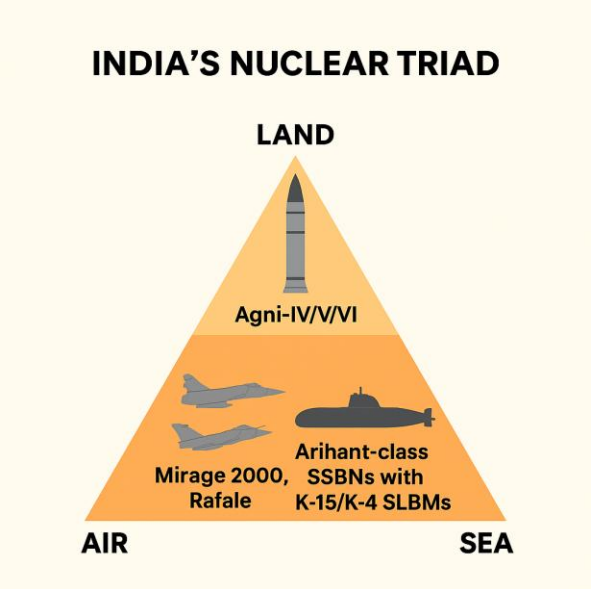
India's nuclear doctrine represents the highest tier of its national security strategy—dealing with existential threats where state survival itself is at stake. Formally articulated in January 2003, drawing upon the Draft Nuclear Doctrine of 1999, it rests on two central pillars: credible minimum deterrence and No First Use (NFU). The doctrine envisions nuclear weapons not as tools of warfighting, but as retaliatory instruments to prevent coercion or blackmail.



While the 2003 doctrine remains the last official statement, subsequent political signals, strategic debates, and technological advances—particularly in the decade after 2014—have hinted at subtle but important evolution. Analysts describe this as India's "new nuclear thinking": continuity with adaptability, designed to manage a shifting security environment.

b. 2003 Nuclear Doctrine – Core Tenets

The official doctrine released in January 2003 contained six foundational principles:



- **Credible Minimum Deterrence:** Maintain only the arsenal required for assured retaliation, avoiding an arms race.
- **No First Use (NFU):** Nuclear weapons would be used only in retaliation against a nuclear strike on India or Indian forces.
- **Massive Retaliation:** Any nuclear attack on India would invite a punitive response designed to inflict "unacceptable damage."
- **Non-Use against Non-Nuclear States:** India pledged not to employ nuclear weapons against NPT-compliant non-nuclear states.
- **Civilian Political Control:** Ultimate authority rests with the Nuclear Command Authority (NCA) chaired by the Prime Minister.
- **Second-Strike Capability:** Survivability of the arsenal through a triad of land-, air-, and sea-based systems to ensure assured retaliation.

c. Possible Evolution Since 2003

Though no formal revision has been issued, several trends point to doctrinal adaptation:

Area	2003 Position	Evolving Indicators
NFU Policy	Firm commitment to NFU	Remarks by defence ministers (2016, 2019) hinted NFU could be conditional in "circumstances."
Response Strategy	Massive retaliation, even against tactical nuclear use	Strategic debate on graded retaliation to avoid disproportionate escalation.
China Focus	Primarily Pakistan-centric; China acknowledged later	Explicit two-front deterrence posture now recognised.
Sea-Based Deterrent	Aspirational	Operationalised with Arihant-class SSBN patrols, strengthening survivability.
Counterforce Debate	Emphasis on counter-value targeting (cities)	Strategic writings discuss counterforce options in extreme scenarios.

d. Drivers of Evolution

Several developments have pressured India to adapt its doctrine:

- **Pakistan's Tactical Nuclear Weapons:** The Nasr (Hatf-IX) short-range system challenges the logic of India's "massive retaliation."
- **China's Expanding Arsenal:** MIRVs, hypersonic glide vehicles, and ASAT capabilities complicate deterrence stability.
- **Technological Advances in India:** Deployment of Agni-V/VI, MIRV capability, precision strike systems, and an operational sea-based deterrent.
- **Political Signalling:** Ambiguity in NFU statements strengthens deterrence by complicating adversary calculations.

e. Doctrinal Pillars – Current Understanding

Despite ongoing debate, India's nuclear posture still revolves around three enduring pillars:

- **Credible Minimum Deterrence:** Avoiding open-ended nuclear arms races while retaining effective deterrence.
- **Assured Retaliation:** Ensuring no adversary can use nuclear coercion without risking devastating response.
- **Survivability of the Nuclear Triad:**
    - **Land:** Agni-series ballistic missiles.
    - **Air:** Nuclear-capable aircraft (Mirage-2000, Rafale).
    - **Sea:** Arihant-class SSBNs armed with K-series SLBMs, ensuring a secure second strike.

f. Internal Security and Strategic Implications

- **Deterrence Stability:** Provides a shield against nuclear blackmail by adversaries.
- **Escalation Control:** NFU enhances India's global image as a responsible nuclear power.
- **Crisis Signalling:** Ambiguity around NFU strengthens deterrence but risks misperception and miscalculation.
- **Cyber & Space Security:** Command-and-control systems must be shielded from cyber intrusions, EMPs, and ASAT attacks.

g. Challenges and Debates

- **Credibility of NFU:** Adversary doubts weaken its stabilising value; China and Pakistan remain sceptical.
- **Two-Front Preparedness:** Simultaneous China–Pakistan nuclear coercion presents unique challenges.
- **Civil–Military Decision Cycle:** Civilian control must coexist with timely response mechanisms in high-speed crises.
- **Survivability:** Adversaries' precision-strike capabilities require India to invest in dispersal, concealment, and redundancy.

Conclusion

India's nuclear doctrine remains formally anchored in 2003 principles, yet its interpretation has evolved. The bedrock pillars of credible minimum deterrence and assured retaliation remain intact, but recent signals suggest calibrated flexibility—especially regarding NFU and the possibility of counterforce in extreme circumstances.

In essence, India seeks to maintain stability while denying adversaries the ability to exploit ambiguity or technological superiority. Its nuclear posture is therefore less about fighting wars and more about

psychological assurance—convincing adversaries that aggression will always invite unacceptable consequences.

As one strategist aptly observed: *"Deterrence works best when your adversary is never certain what you will do—but always certain you can."*

Epilogue: The Integrated Security Challenge

India's security environment today is not shaped by a single enemy or battlefield, but by the convergence of diverse threats—ethnic violence and insurgencies, illegal migration and narcotics, drones and cyberattacks, piracy and terrorism, and the shadow of nuclear deterrence. These challenges are distinct yet interconnected: the OGW in Kashmir, the trafficker in the Northeast, the botnet operator in cyberspace, and the Chinese missile on the horizon all represent different facets of the same problem—the continuous probing of India's resilience. The line between internal and external threats has blurred, as hybrid warfare ensures that propaganda, infiltration, and digital disruption merge seamlessly into one another.

Three broad lessons stand out. First, security must be multi-layered. A border fence is meaningless without local community trust; counter-terror operations cannot succeed without dismantling OGW networks; and nuclear deterrence is only credible if satellites and command systems are cyber-secure. Military force, diplomacy, technology, development, and social cohesion must work together as reinforcing layers.

Second, resilience is as critical as strength. Drones may be shot down and hackers repelled, but unless systems adapt and improve after every breach, vulnerabilities persist. The Risk Management Framework in cyber defence, rehabilitation in counter-insurgency, and phased demobilisation in the Northeast all reflect the same principle: security is a cycle of anticipation, response, and renewal.

Third, India's diversity is both challenge and strength. Ethnic divisions and refugee pressures can trigger violence and insurgency, but when managed inclusively, diversity becomes a source of resilience. National security cannot be separated from social cohesion and constitutional values—citizens must feel ownership of the state for stability to endure.

Looking ahead, India must navigate great power competition with China and Pakistan, insurgencies in its borderlands, and digital disruptions that threaten its economic backbone. Adversaries will continue to exploit seams—geographic, social, and technological. The task for India is to close these gaps without closing society, to build strength without sacrificing liberty, and to ensure that its rise as a global power rests on internal stability.

As Kautilya warned, a ruler who neglects border security loses sovereignty; in today's world, that maxim extends to cyberspace, finance, and social cohesion. Security is not an end in itself but an enabler—the shield that protects India's growth, democracy, and global aspirations.

"The true strength of a nation lies not in the weapons it wields, but in the resilience of its people and the unity of its purpose."

Internal Security PYQs (2021-2025)

2025

Q. Terrorism is a global scourge. How has it manifested in India? Elaborate with contemporary examples. What are the counter measures adopted by the State? Explain. (Answer in 150 words)

Q. The Government of India recently stated that Left Wing Extremism (LWE) will be eliminated by 2026. What do you understand by LWE and how are the people affected by it? What measures have been taken by the government to eliminate LWE? (Answer in 150 words)

Q. What are the major challenges to internal security and peace process in the North-Eastern States? Map the various peace accords and agreements initiated by the government in the past decade. (Answer in 250 words)

Q. Why is maritime security vital to protect India's sea trade? Discuss maritime and coastal security challenges and the way forward. (Answer in 250 words)

2024

Q. Social media and encrypting messaging services pose a serious security challenge. What measures have been adopted at various levels to address the security implications of social media? Also suggest any other remedies to address the problem. (Answer in 250 words)

Q. India has a long and troubled border with China and Pakistan fraught with contentious issues. Examine the conflicting issues and security challenges along the border. Also give out the development being undertaken in these areas under the Border Area Development Programme (BADP) and Border Infrastructure and Management (BIM) Scheme. (Answer in 250 words)

Q. Explain how narco-terrorism has emerged as a serious threat across the country. Suggest suitable measures to counter narco-terrorism. (Answer in 150 words)

2023

Q. Give out the major sources of terror funding in India and efforts being made to curtail these sources. In the light of this, also discuss the aim and objective of the 'No Money for Terror [NMFT]' Conference recently held at New Delhi in November 2022. (Answer in 250 words)

Q. What are the internal security challenges being faced by India? Give out the role of Central Intelligence and Investigative Agencies tasked to counter such threats. (Answer in 250 words)

Q. The use of unmanned aerial vehicles (UAVs) by our adversaries across the borders to ferry arms/ammunitions, drugs, etc., is a serious threat to the internal security. Comment on the measures being taken to tackle this threat. (Answer in 150 words)

Q. Winning of 'Hearts and Minds' in terrorism affected areas is an essential step in restoring the trust of the population. Discuss the measures adopted by the Government in this respect as part of the conflict resolution in Jammu and Kashmir. (Answer in 150 words)

2022

Q. Naxalism is a social, economic and developmental issue manifesting as a violent internal security threat. In this context, discuss the emerging issues gest a multilayered strategy to tackle the menace of Naxalism. (Answer in 250 words)

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. (Answer in 250 words)

Q. What are the maritime security challenges in India ? Discuss the organisational, technical and procedural initiatives taken to improve the maritime security. (Answer in 150 words)

Q. Discuss the types of organised crimes. Describe the linkages between terrorists and organised crime that exist at the national and transnational levels. (Answer in 150 words)

2021

Q. Analyse the complexity and intensity of terrorism, its causes, linkages and obnoxious nexus. Also suggest measures required to be taken to eradicate the menace of terrorism. (Answer in 250 words)

Q. Analyse the multidimensıonal challenges posed by external state and non-state actors, to the internal security of India. Also discuss measures required to be taken to combat these threats. (Answer in 250 words)

Q. Keeping in view India's internal security, analyse the impact of cross-border cyber attacks. Also discuss defensive measures against these sophisticated attacks. (Answer in 150 words)

Q. Discuss how emerging technologies and globalisation contribute to money laundering. Elaborate measures to tackle the problem of money laundering both at national and international levels. (Answer in 150 words)

Internal Security PYQs Analysis (2021–2025)

a. Trend Summary: Weightage and Frequency

Year	No. of Questions	Total Marks	Type (10/15)	Subtopic Focus
2021	4	50	2×10 + 2×15	Terrorism, External Actors, Cyber Threats, Money Laundering
2022	4	50	2×10 + 2×15	Naxalism, Cybersecurity, Maritime, Organised Crime
2023	4	50	2×10 + 2×15	Terror Funding, Intelligence, Drones, J&K Peacebuilding
2024	3	40	1×10 + 2×15	Narco-Terrorism, Borders, Social Media
2025	4	50	2×10 + 2×15	Terrorism, LWE, North-East, Maritime Security

Across this five-year period, Internal Security has displayed remarkable consistency, averaging around four questions and 48–50 marks annually. The thematic focus has evolved from conventional threats to technological, transnational, and asymmetric warfare—anchoring it as a steady, high-yield pillar of GS Paper 3.

This continuity reflects how the paper mirrors India's changing threat spectrum—from territorial to digital and from kinetic to financial domains.

b. Nature of Questions

Type	Description	Dominant Years
Conceptual	Foundational definitions—terrorism, organised crime, cyber threats	2021–22
Applied	Use of technology in warfare, drones, encryption, AI	2023–25
Analytical	Peacebuilding, governance reforms, conflict resolution	2023–25

The dominant tilt is applied and analytical. UPSC now expects aspirants to connect theory with institutional responses, demonstrating how definitions translate into actionable frameworks and governance mechanisms.

c. Core Themes and Subtopics

Core Theme	Example PYQs	Frequency	Trend	Relevance
Terrorism & Counter-Terrorism	Funding networks, J&K, LWE, NMFT	8	Rising	Very High
Cybersecurity & Emerging Tech	Cross-border cyberattacks, AI-based risks	5	Rising	Very High
Border & Maritime Security	BADP, Indo-Pacific routes, sea-lane protection	5	Steady	High
Organised Crime & Narco Nexus	Narco-terror, crime–terror convergence	3	Emerging	Medium–High

Core Theme	Example PYQs	Frequency	Trend	Relevance
Insurgency & Left-Wing Extremism	Naxal dynamics, North-East reconciliation	4	Rising	Very High
Information Warfare & Social Media	Propaganda ecosystems, encrypted messaging	2	New Focus	Emerging

Together, these clusters define the modern threat triad—terrorism, technology, and transnational crime—which dominates the contemporary internal security landscape.

d. Current Affairs and Real-Event Anchors

Year	Real Event	Theme Tested
2021	Pegasus revelations and cyber intrusions	Cross-border cyber espionage
2022	Draft National Cyber Security Strategy; LWE decline	Digital policy and internal stabilisation
2023	No Money for Terror (NMFT) conference; drone drops in Punjab	Terror financing and UAV proliferation
2024	Narco routes via maritime corridors	Narco-terror architecture
2025	North-East peace accords; Maritime Security Review	Regional reconciliation and coastal resilience

UPSC tends to align its questions with recent national and global policy developments, drawing from MHA reports, FATF proceedings, and strategic reviews rather than news events alone.

e. Interlinkages with Other Papers

Paper	Example	Focus
GS Paper 2	Peace accords, North-East governance	Centre–state coordination, federal security
GS Paper 3	Cyber threats, narco networks	Science, economy, and internal stability
GS Paper 4	Policing ethics, surveillance dilemmas	Proportionality, accountability, privacy
Essay Paper	National security & social cohesion	Holistic analysis of internal order

Internal Security thus serves as the conceptual and operational hinge connecting technology, governance, and ethics—making it essential for integrated GS preparation.

f. Evolution of Question Trends

Shift	Example
Traditional → Hybrid Warfare	From generic terrorism to UAVs, narco-terror, and cyber conflict
State-centric → People-centric	From eradication to hearts-and-minds campaigns
Physical → Digital Domains	From border incursions to encrypted ecosystems

Shift	Example
India-only → Transnational Frames	From LWE silos to global terror-finance linkages

UPSC now tests awareness of multi-domain conflict, where digital, financial, informational, and territorial dimensions intersect.

g. Hidden or Abstract Phrases

Phrase	Underlying Theme
"Global Scourge"	Transnational terrorism and international cooperation
"Hearts and Minds"	Human-centric counter-insurgency
"Encrypted Services"	Privacy versus lawful access debate
"No Money for Terror"	Global financial intelligence coordination
"Peace Process"	Reintegration and sequencing of reconciliation efforts

Recognising such abstract cues helps candidates unpack policy-oriented questions and frame nuanced institutional solutions.

h. Frameworks and Institutional Anchors

Category	Frameworks and Institutions
Acts & Strategies	UAPA, NDPS Act, National Cyber Security Strategy (Draft 2022), National Maritime Security Strategy (2023)
Agencies	NIA, IB, NCB, NTRO, MHA, NSCS, NDRF (dual-role utility)
Operations	SAMADHAN (LWE), SAGAR (maritime), MADAD (coastal), Blue Star-II (anti-drone)
Global Cooperation	FATF, NMFT, INTERPOL, UNODC, BIMSTEC Security Forum

The trend underscores India's institutional consolidation, where legal frameworks, inter-agency synergy, and global cooperation collectively define modern security architecture.

i. Comparative and Strategic Framing

Contrast	Illustration
Internal vs External	Internal stability shaped by external infiltration modes
Tech vs Human Intelligence	AI and drones supplement but cannot replace fieldcraft
Security vs Liberty	Encryption debates reveal democratic balancing acts
Centre vs State Roles	Cooperative federalism critical in LWE & NE regions
Maritime vs Continental Fronts	Indo-Pacific vigilance reinforces homeland security

This comparative framing allows aspirants to demonstrate analytical range, balancing national security imperatives with civil liberties and governance efficiency.

j. Predictive Insights: 2025–26

Probable Theme	Rationale
AI-enabled Hybrid Warfare	Rapid convergence of AI, drones, and surveillance tech
Cyber-enabled Terror Finance & Dark Web	FATF focus on digital anonymity and crypto finance
Border Tech & AI Surveillance	Deployment of integrated command grids
Narco Routes via Sea & NE Corridors	Persistent trafficking trends post-2024
Deepfakes & Information Warfare	Threats to democratic discourse and perception security

The upcoming cycles may prioritise AI–security intersection, narco–terror linkages, and cognitive warfare, marking the frontier of India's internal security discourse.

k. Answer Writing Takeaways

Element	Strategy
Answer Enrichers	Cite Acts (UAPA, NDPS), schemes (SAMADHAN, SAGAR), global platforms (FATF, NMFT).
Pitfalls	Avoid generic moralism; employ institutional vocabulary.
Structure	a. Define → b. Analyse threats → c. Explain response matrix → d. Suggest reforms.
Visual Aid	Use a "Threat–Response Matrix" diagram mapping traditional, non-traditional, and emerging threats.

High-quality answers maintain precision, inter-agency awareness, and policy realism, aligning operational insight with ethical considerations.

l. Executive Summary

Parameter	Insight
Average Marks (2021–25)	~48 marks/year
Trend	Stable with technological evolution
Dominant Type	Applied and Analytical
Core Focus	Hybrid threats—terror, cyber, border
Predicted 2026 Focus	AI warfare, narco-terror, cyber governance

Conclusion

Between 2021 and 2025, Internal Security questions evolved from conventional counter-terrorism to a hybrid, technology-driven paradigm. The paper now demands a multi-dimensional grasp of law, technology, finance, and governance.
Scoring well depends on demonstrating precision in terminology, clarity in inter-agency architecture, and pragmatic vision in recommendations.

Acknowledgments

Behind every page of PrepAlpine lies a collective of educators, civil servants, researchers, and mentors — united by a shared belief that clarity, integrity, and precision can redefine UPSC preparation.

This work is the outcome of months of academic collaboration across multiple content verticals — each bringing its own discipline and expertise to ensure that learning remains authentic, structured, and exam-aligned.

Academic & Content Leadership

To the Head of Content Development — a senior civil servant whose academic vision and policy insight anchor the intellectual core of PrepAlpine content.
Your leadership ensures that every topic reflects administrative realism, conceptual rigour, and syllabus-aligned relevance.

Civil Servant Contributors

To our contributing officers and administrators — for adding rare authenticity through real-world case studies, governance perspectives, and ethical nuance.
Your inputs elevate the material beyond preparation — turning it into a bridge between policy and practice.

Content Research & Review Team

For meticulously gathering, structuring, and validating material from diverse authentic sources, and for upholding the highest standards of factual accuracy and conceptual depth.
Your collective effort transforms data into understanding and ensures that PrepAlpine content remains both exam-ready and intellectually rich.

Content Creation & Enhancement Team

For crafting lucid explanations and visuals that embody the PrepAlpine Writing Framework — blending academic rigour with learner-centric clarity.
Your diagrams, flowcharts, and design coherence make complex ideas accessible and memorable.

Mentorship & SME Coordination

To the mentors and subject-matter experts who continuously refine our frameworks through feedback, reviews, and conceptual discussions.
Your interaction between field insight and pedagogy keeps our content dynamic, relevant, and aligned with evolving UPSC standards.

Editorial & Proofreading Team

For your line-by-line precision — refining tone, coherence, and academic consistency while safeguarding accuracy.
Your quiet diligence ensures that every paragraph meets the PrepAlpine benchmark of quality and credibility.

Each of you represents a vital link in the PrepAlpine Content Chain — thinkers, writers, reviewers, and mentors working together to ensure that every page upholds our founding principle:
Preparation must meet Precision.

— **The PrepAlpine Team**
November 2025

Reader's Note

Dear Aspirant,

This document is part of the *PrepAlpine General Studies Series* — created to bring clarity, structure, and precision to your UPSC learning journey across all GS subjects.

Each page reflects the *PrepAlpine* vision: to make preparation intelligent, collaborative, and evolution-based — where content, mentorship, and community constantly refine one another.

1. Orientation & Purpose

This compilation has been curated from the UPSC Mains perspective, emphasizing:

- Conceptual clarity over superficial memorization,
- Analytical depth across GS papers, and
- Interlinkages between static and current topics (e.g., linking History with Polity, Geography with Environment, Economy with Society).

While designed primarily for Mains, its layered explanations also make it a valuable asset for Prelims, Essays, and Interviews.

2. Content Depth & Flexibility

Content length varies according to topic relevance, conceptual density, and exam weightage.
You are encouraged to use any free LLM tool (like ChatGPT or Gemini) to adapt content — whether for deeper exploration, quick summaries, or visual restructuring (lists ↔ paragraphs ↔ tables).

The *PrepAlpine* approach focuses on understanding → retention → application, rather than rote learning.

3. Format & Adaptability

This compilation integrates paragraphs, lists, tables, and infographics — each serving a distinct learning purpose.
However, if you prefer a particular presentation style, you can easily use free Large Language Models (LLMs) like *ChatGPT* or *Gemini* to restructure and personalize the content.

For example, you can:

- Convert formats: Instantly transform lists ↔ paragraphs ↔ tables to match your preferred way of reading or revising.
- Expand or Condense: Ask the LLM to elaborate on complex sections for conceptual depth or summarize lengthy topics for quick revision.
- Customize Visual Flow: Reorganize explanations, add examples, or even merge related sections for integrated understanding.

This ensures every aspirant can adapt *PrepAlpine* material to their own learning rhythm, visual preference, and revision speed — without losing the structure, coherence, or clarity of the original content.

4. Continuous Upgradation (Colour-Coded Editions)

In line with our community-driven model, the *PrepAlpine* team continuously refines and expands this content based on aspirant feedback shared through our Discord community.

When aspirants highlight missing topics or underdeveloped sections, we commit to releasing an updated, colour-coded edition every 3–4 months, where:

- 🟢 New Additions are clearly marked for easy migration.
- 🟡 Expanded/Updated Sections are highlighted for focused review.
- 🔵 Revised Data or Case Studies are timestamped for transparency.

This ensures you can seamlessly transition from older to newer versions without confusion or redundancy.

5. Join the PrepAlpine Discord Community

Be part of India's Smartest UPSC Peer Ecosystem → https://discord.gg/yrcDpXxv

What You'll Experience:

- Peer-to-Peer Discussions: Subject-wise channels for Ethics, GS, Optional and more.
- Focused Study Circles: Deep-dive groups for optional subjects and GS themes.
- Insight Threads: Collaborative notes, doubt resolutions, and peer-reviewed clarity.
- Community Sessions: "Open Mic" days for sharing strategies and lessons from the UPSC journey.
- Evolving Learning Culture: 100% peer-driven, serious yet supportive — where learning grows through discussion, not noise.

"From Isolation to Interaction — Learn the UPSC Way, the Smart Way."

6. Suggest Topics & Shape Future Editions

Your feedback directly shapes the *PrepAlpine GS Series.*
If you identify any missing topic, conceptual gap, or new policy issue, share it in the "Suggestions" channel on our Discord.

Our editorial team reviews all community inputs before each quarterly edition, ensuring that future versions are richer, sharper, and more inclusive.

7. The PrepAlpine Vision

This compilation embodies our core philosophy:

Better Content. Smarter Mentorship. Intelligent Preparation.

By combining evolving content, authentic mentorship, and collaborative community learning, the *PrepAlpine Series* aims to transform UPSC preparation from solitary reading into a living, evolving, and intelligent ecosystem.

With best wishes for your journey ahead — stay curious, stay consistent, and keep evolving.
– Team PrepAlpine