Internal Security

MPSC Mains

General Studies III

Class Notes

PRAYAAS

Published by

PRAYAAS Education

CTS No, 1262/B, Plot No.594B,
Office 301A, 301, Second Floor,
Starling Plaza, J.M. Road, Pune

+91 7378743031 / +91 7767073031

MPSC MAINS

Internal Security

GENERAL STUDIES - III

(Class Notes)

Year 2025-26

Features of Internal Security Notes (MPSC Focused)

1. Conceptual Clarity through Key Terms

- Concise definitions of 100+ critical terms (e.g., cyber terrorism, hybrid warfare, left-wing extremism, coastal security, etc.)
- Linked with real-world examples and recent policy updates
- Keywords crafted for direct use in answers and introductions

---

2. Point-Wise Topic Breakdown

- All syllabus topics (both static and dynamic) broken down into easy-to-absorb bullet points
- Ideal for quick revision, answer writing, and retention
- UPSC-optimized structure for faster recall and crisp presentation

---

3. Syllabus Mapping + Mains-Oriented Categorization

- All content aligned with GS Paper-III syllabus
- Subtopics tagged with their relevance: National Security, Cybersecurity, Extremism, Border Management, etc.

---

4. Current Affairs Integration

- Case studies and examples from post-2023 developments (e.g., recent data breaches, AI in surveillance, drone attacks, etc.)
- Government schemes, acts, and committee recommendations added where relevant

5. Answer Writing Enablers

- Mini-notes under each topic tailored for 10-marker and 15-marker answers
- Embedded with directive-based framing: Examine, Analyze, Critically evaluate, etc.

- Sample intro and conclusion templates included

---

6. Revision Friendly & Exam Ready

- Structured for pre-mains revision in 5–6 hours
- QR codes or index tags for cross-referencing key topics (optional feature if you're digitizing)
- Handy for open-book tests and quick note-adding

---

7. Value Addition Booklet

- Exclusive "Ready Reckoner" pages: Quotes, Committees, Supreme Court Judgments, and IR links to Internal Security

INDEX

1 UNIT

Linkages Between Development and Spread of Extremism

Navigating the Syllabus: What You Need to Know

Linkages between Development and Spread of Extremism.

- What is Extremism..??
- Factors Responsible for spread of Extremism
- Challenges to internal security due to spread of extremism
- Steps needed to reduce the spread of Extremism

UPSC Previous Year Questions

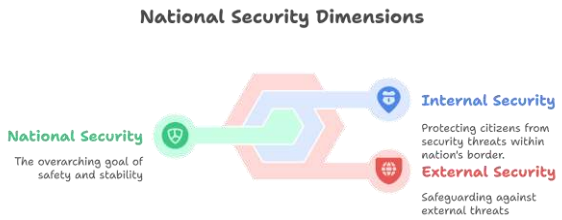
Question	Nature of Question	Core Demand
Winning of 'Hearts and Minds' in terrorism-affected areas is an essential step in restoring the trust of the population. Discuss the measures adopted by the Government in this respect as part of the conflict resolution in Jammu and Kashmir. (2023)	Conflict Resolution + Policy Measures	Discuss trust-building and outreach measures taken by government in J&K.
Naxalism is a social, economic and developmental issue manifesting as a violent internal security threat. In this context, discuss the emerging issues and a multilayered strategy to tackle the menace. (2022)	Internal Security + Governance	Discuss emerging issues and outline multilayered strategy to counter Naxalism.
What are the determinants of left-wing extremism in Eastern India? What strategy should government, civil administration, and security forces adopt? (2020)	Root Causes + Strategic Response	Identify causes of LWE and recommend strategies for state and security forces.

LWE is showing a downward trend, but still affects many parts of the country. Briefly explain the Government of India's approach. (2018)	Trend-Based + Policy-Oriented	Explain government's approach to tackle LWE in current scenario.
Mob violence is emerging as a serious law and order problem. Analyze causes and consequences with examples. (2017)	Social Issue + Law & Order	Analyze reasons and consequences of mob violence with relevant examples.
Drives for large industries in backward areas have isolated tribals and farmers. With Malkangiri and Naxalbari as focus, discuss corrective strategies. (2015)	Development vs Alienation	Suggest corrective strategies to mainstream affected citizens in LWE zones.
Article 244 relates to Scheduled Areas. Analyze impact of non-implementation of Fifth Schedule on LWE. (2013)	Constitutional + Governance Failure	Analyze how neglect of Fifth Schedule provisions contributes to LWE growth.

1 Introduction to Security

Introduction

Security, in the context of a nation-state, refers to the protection of its sovereignty, territorial integrity, and core national interests from threats. It encompasses both **internal security**—dealing with challenges like terrorism, insurgency, and cybercrime within borders—and **external security**, which involves safeguarding against foreign aggression, cross-border conflicts, and geopolitical threats. Together, they form the foundation of national stability and strategic autonomy.



What is Internal security ?

- Internal Security refers to the capacity of the state to maintain peace and stability within its borders by safeguarding against threats that originate from within—whether in the form of terrorism, insurgency, communal violence, cybercrime, or organized crime.
- It ensures the protection of life, property, democratic institutions, and the rule of law, thereby fostering a secure environment for governance and development.

Key Components of Internal Security

Component	Description
Law Enforcement	Enforcement of law and order through police forces and paramilitary agencies.
Intelligence & Surveillance	Gathering actionable intelligence to prevent internal threats; includes HUMINT and TECHINT.
Border Management	Securing land and maritime boundaries to prevent cross-border infiltration, smuggling, and trafficking.
Counterterrorism	Measures to detect, prevent, and dismantle terrorist networks and radicalization processes.
Cybersecurity	Safeguarding digital infrastructure from cyber attacks, data breaches, and online radicalization.
Emergency Preparedness & Disaster Response	Planning for and responding to natural and man-made disasters, including pandemics.
Community Policing	Promoting trust and cooperation between police and citizens to enhance local intelligence and reduce alienation.
Legal-Institutional Framework	Enactment and enforcement of laws like UAPA, NSA, and NIA Act; supported by judiciary and oversight mechanisms.

What is External Security

- External security refers to the protection of a nation from threats and aggression originating outside its borders.
- It involves defending territorial sovereignty, maintaining strategic deterrence, and ensuring national interests in the global arena.
- External security is crucial not only for protecting geographical boundaries but also for securing maritime, aerial, and space domains.

Key Components of External Security

Component	Description
Military Defence	Strengthening armed forces to deter and repel external aggression. Includes modernization of the Army, Navy, and Air Force.
Strategic Deterrence	Maintaining credible nuclear and missile capabilities (e.g.,

	through the Nuclear Triad) to deter adversaries.
Border Security	Vigilance along land, maritime, and aerial boundaries, particularly in conflict-prone regions like LOC, LAC.
Defence Diplomacy	Building strategic partnerships (e.g., QUAD, Indo-US defence agreements) and military cooperation to bolster regional security.
Maritime Security	Securing sea lanes of communication (SLOCs), Exclusive Economic Zone (EEZ), and countering piracy or naval threats.
Space & Cyber Defence	Protecting critical space infrastructure and cyberspace from espionage, sabotage, and cyber warfare.
Intelligence Operations	Gathering transnational intelligence to pre-empt external threats, in collaboration with international agencies.
Defence Production & Self-Reliance	Reducing import dependency through initiatives like 'Atmanirbhar Bharat' and promoting indigenous defence manufacturing.

Difference Between Internal and External Security

Aspect	Internal Security	External Security
Definition	Protection from threats arising **within the country** (e.g., insurgency, riots).	Protection from threats originating **outside the country** (e.g., war, invasion).
Main Threats	Terrorism, left-wing extremism, communal violence, organized crime, cyber threats.	Cross-border terrorism, military aggression, territorial disputes, espionage.
Agencies Involved	Police forces, Intelligence Bureau (IB), Central Armed Police Forces (CAPFs).	Armed Forces (Army, Navy, Air Force), RAW, DRDO, Strategic Forces Command.
Jurisdiction	Operates primarily under **Ministry of Home Affairs (MHA)**.	Operates under **Ministry of Defence (MoD)** and Ministry of External Affairs (MEA).
Nature of Threat	Non-conventional, often involves **non-state actors** and internal dissidence.	Conventional and non-conventional, involves **state and non-state actors**.
Legal Framework	IPC, CrPC, UAPA, NSA, NIA Act, etc.	Defence Services Acts, National Security Act, International Treaties, Geneva Conventions.
Example	26/11 Mumbai attacks, Maoist	Kargil War (1999), 2020 Galwan Valley clash, Indo-Pak wars.

	insurgency, 2020 Delhi riots.	
Approach	Community engagement, intelligence, policing, legal action, cyber surveillance.	Military preparedness, diplomacy, defence alliances, strategic deterrence.
Impact Zone	Mostly confined to internal regions and civilian population.	Border areas, maritime zones, and national defence infrastructure.

2 Linkage Between Development and Extremism

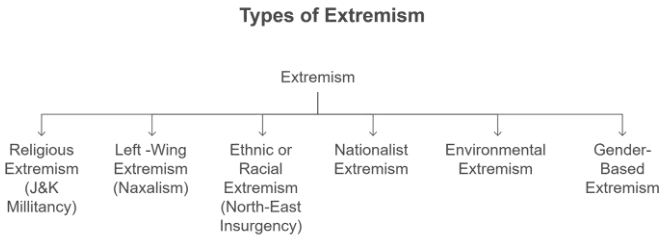
Introduction:

Extremism in India, particularly in regions affected by Left-Wing Extremism and insurgencies, is not merely a law and order issue but deeply rooted in the failure of equitable development. When governance deficits, socio-economic deprivation, and exclusion from mainstream progress persist, disillusionment sets in—creating fertile ground for extremist ideologies. Thus, the absence of development becomes both a cause and consequence of internal conflict, making it imperative to address the developmental roots of extremism alongside security responses.

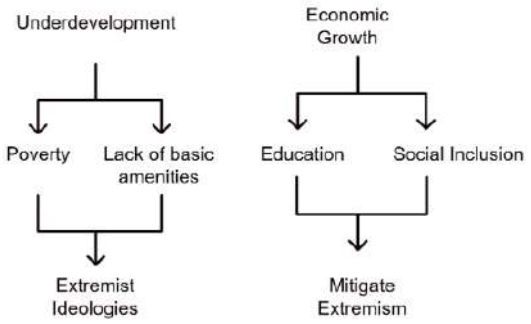
What is meant by Extremism?

- Extremism refers to beliefs, ideologies, or actions that significantly deviate from accepted societal norms and often reject the principles of democracy, pluralism, and peaceful engagement.
- It often manifests through **intolerance, violence, or the use of unlawful means** to achieve objectives, and seeks to disrupt the existing socio-political order.
- In the Indian context, extremism includes movements like **Left-Wing Extremism (LWE), religious radicalism, and ethno-nationalist insurgencies** that challenge the authority of the state and threaten internal security.
- As per **Peter T. Coleman and Andrea Bartoli**:
  - *"Extremism is a complex phenomenon... most simply, it can be defined as activities (beliefs, attitudes, feelings, actions, strategies) of a character far removed from the ordinary. In conflict settings, it manifests as a severe form of conflict engagement. However, the labeling of activities, people, and groups as 'extremist', and the defining of what is 'ordinary' in any setting is always a subjective and political matter."*

Various types of Extremism



How Development and Extremism are Linked

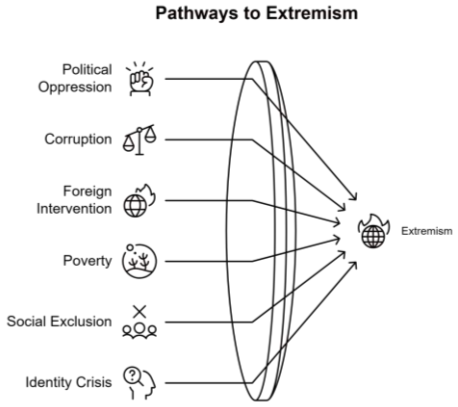


Extremism in India, particularly in Left-Wing Extremism (LWE)-affected regions, is not just a security concern but deeply rooted in the **failures of inclusive development, unresponsive governance, and socio-economic deprivation**. The nexus between **underdevelopment and extremism** manifests as a **self-reinforcing cycle** where the absence of justice and opportunity fosters alienation and fuels radical mobilization.

- **Resource Extraction Without Local Benefit**
  - Many LWE-affected districts are mineral-rich but remain development-poor. Local communities are often displaced for mining or industrial projects without fair compensation or rehabilitation.
  - *Example:* In **Dantewada and Bastar (Chhattisgarh)**—districts rich in iron ore—tribals have been repeatedly displaced by projects like NMDC mining, while human development indicators remain among the lowest in India (NFHS-5, 2021: tribal literacy in Bastar <50%; severe anemia among women ~28%).
  - This disconnect between **economic growth and human development** fuels resentment and strengthens extremist narratives about "exploitation by the state."
- **Alienation Due to Land Insecurity and Poor Forest Rights Implementation**

- Land is both a source of identity and livelihood, especially for Adivasi populations. When displaced without proper legal support, people feel betrayed.
- *Example:* A 2022 report by the **Ministry of Tribal Affairs** noted that **over 47% of forest rights claims** under the Forest Rights Act (2006) in Jharkhand and Odisha were rejected—often without proper documentation or support.
- Extremist groups like Maoists position themselves as defenders of tribal land and rights, gaining support in areas where **state institutions are viewed as exploiters.**

- **Governance Vacuum and Lack of Basic Services**
  - Development is not only about GDP—it is about **state presence, justice, and access to services**.
  - *Example:* As of 2020, only **about 65% of the planned roads under the Road Requirement Plan-I (RRPI)** for LWE areas were completed (as per MHA reply in Lok Sabha). Inaccessible terrain and poor roads delay policing and development delivery.
  - In such power vacuums, Maoists run parallel governance structures—resolving disputes, collecting taxes, and holding "Jan Adalats"—filling a void left by the state.
- **Youth Disillusionment Due to Unemployment and Lack of Skills**
  - In backward regions, **lack of jobs and vocational training** leads to frustration among youth, who are then easily drawn into extremist networks that offer purpose and belonging.
  - *Example:* According to the **NITI Aayog's 2021 review** of Aspirational Districts, **Koraput (Odisha)** and **Latehar (Jharkhand)** reported youth unemployment rates above **20%**, with skill training enrolments below the national average.
  - This **aspirational vacuum**, when combined with a sense of historical neglect, creates fertile ground for radicalization.
- **Absence of Participatory and Culturally Sensitive Development**
  - Development imposed from the top, without local participation or cultural sensitivity, leads to rejection and resistance.
  - *Example:* In **Andhra Pradesh's tribal belt**, several industrial corridors were planned without Gram Sabha consultation under PESA and FRA provisions. The result was mass protests, some of which were exploited by Maoists to consolidate support.
  - When **tribal voices are ignored**, development is seen not as empowerment but as imposition.
- **Ineffective Grievance Redress and Delayed Justice**
  - When people do not have access to timely justice, they resort to alternative systems, including extremist channels.
  - *Example:* In regions like **Sukma and Malkangiri**, pendency of land cases and delayed implementation of MGNREGA wages have been reported in CAG audits (2022), leading to local frustration.



  - Maoist "courts" exploit this failure by offering swift resolutions, even if through fear or parallel authority.

Categorization of Extremism in India: Developmental Linkages

Type of Extremism	Region	Primary Drivers	Development Linkage	Remarks
1. Left-Wing Extremism (LWE) *(Naxal-Maoist Insurgency)*	Central & Eastern India (Chhattisgarh, Jharkhand, Odisha,	Land alienation, tribal displacement, exploitation, state neglect	**Strong** – Rooted in socio-economic inequality and underdevelopment	Described by PM Manmohan Singh as "India's greatest internal security threat"

	Maharashtra, etc.)			
2. Ethno-Nationalist Insurgency *(North-East India)*	North-East India (Nagaland, Manipur, Assam, etc.)	Ethnic identity assertion, demand for political autonomy, perceived marginalization	**Moderate to Strong** – Fuelled by economic neglect and connectivity gaps	Peace Accords and special constitutional provisions have helped manage it
3. Religious & Separatist Extremism *(Jammu & Kashmir Militancy)*	Jammu & Kashmir	Religious radicalism, cross-border terrorism, secessionist ideology, political alienation	**Indirect/Minimal** – Youth alienation, lack of employment, trust deficit exacerbate the conflict	Development deficit is an **aggravating**, not root cause
4. Urban Extremism / Radicalization	Pan-India (especially metros)	Ideological indoctrination via online platforms, lone wolf attacks, global jihad	**Minimal** – Driven more by ideology than material deprivation	Tackled through cyber surveillance, de-radicalization cells

(We are going to discuss more details about these topics in separate chapters)

3 Left-wing extremism (LWE) or Naxal insurgency

Introduction

- **Left-Wing Extremism (LWE)** refers to ideologies and movements that seek to overthrow the existing democratic and economic structures through violent means, often inspired by Maoist or Marxist-Leninist ideologies.
- In the Indian context, LWE is primarily associated with **Maoist insurgents**, also known as **Naxalites**, who claim to represent the interests of tribal populations, landless laborers, and other marginalized groups.

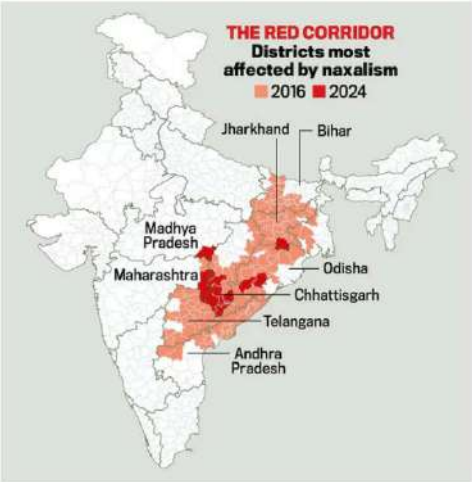
Historical Background Evolution of Left-Wing Extremism

- The term gained prominence post the **1967 Naxalbari uprising** in West Bengal, where a group of peasants led by Charu Majumdar and Kanu Sanyal launched an armed rebellion against feudal landlords and the state, marking the ideological birth of the Naxalite movement.
- Over time, LWE has evolved into a **serious internal security challenge**, particularly in the "Red Corridor" — a region spanning several states including Chhattisgarh, Jharkhand, Odisha, Bihar, Maharashtra, and parts of Andhra Pradesh and Telangana.
- **Evolution of LWE (Post-1967)**

Phase	Key Developments
1970s	Rapid spread in Bihar, Andhra Pradesh, and Kerala. State repression and internal splits weakened the movement.
1980s	Resurgence in Andhra Pradesh under **People's War Group (PWG)**; targeted landlords and police; parallel justice systems created in remote areas.
1990s	Mergers and reconfigurations among extremist groups. Rise of **Maoist Communist Centre (MCC)** in Bihar and Jharkhand.
2004	Merger of **PWG** and **MCC** into the **Communist Party of India (Maoist)** — unified and most potent LWE group.
2005 onwards	Government launches **Salwa Judum (Chhattisgarh)**; large-scale militarization and civilian displacement ensue. CPI (Maoist) expands to 200+ districts.
2010	Government declares LWE the **"biggest internal security threat"** (PM Manmohan Singh); launches **Integrated Action Plan (IAP)** and **SAMADHAN strategy**.
2018–2024	Decline in violence and affected districts due to coordinated security operations, development push, and surrenders. Fewer than **45 districts** affected in 2023 as per MHA.

Geographical Spread of Left-Wing Extremism (LWE)

- Left-Wing Extremism in India is **concentrated in remote, forested, and tribal-dominated regions**, where governance is weak and socio-economic deprivation is acute. The movement has historically spread through what is known as the **"Red Corridor"**.
- **The "Red Corridor"**
  - Refers to the **contiguous belt of LWE-affected districts** running from **central India to the eastern coast**.
  - States majorly affected include:
    - **Chhattisgarh** (especially Bastar region)
    - **Jharkhand**
    - **Odisha** (Koraput, Malkangiri)
    - **Bihar**
    - **Maharashtra** (Gadchiroli)
    - **Telangana** (northern districts)
    - **Andhra Pradesh** (declining influence)
    - **West Bengal** (earlier stronghold, now largely neutralized)



Causes of Left-Wing Extremism (LWE) in India

LWE is often described as a **"reaction to decades of neglect"** in India's tribal and forest regions. It thrives where **governance is weak**, **development is poor**, and **institutional justice is absent**.

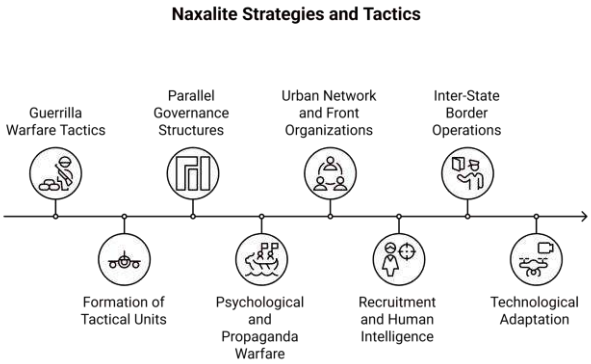
- **Socio-Economic Causes**
  - **Land Alienation and Displacement**: Large-scale land acquisition for mining and infrastructure, often without proper rehabilitation, fuels resentment among tribals.

Case Study: Displacement Due to Mining in Hasdeo Arand, Chhattisgarh

- The **Hasdeo Arand forest**, spread over ~170,000 hectares in Chhattisgarh, is inhabited by tribal communities like the Gonds. Coal mining projects such as the **Parsa East and Kanta Basan (PEKB) block**, operated by Adani Enterprises and Rajasthan Rajya Vidyut Utpadan Nigam Ltd., have led to the **displacement of several villages**.
- Despite the **Forest Rights Act (2006)** requiring Gram Sabha consent, locals allege **violations of procedural rights**, **inadequate compensation**, and **loss of forest-based livelihoods**. The **long-running protests** by tribal communities highlight the failure of inclusive development.
- This unrest has been exploited by **Maoist groups** to mobilize local support, feeding into **LWE narratives of state apathy and corporate exploitation**.

  - **Poverty and Unemployment**: Lack of livelihood options in forest and hilly areas makes the population vulnerable to recruitment by Maoists.
    - *NFHS-5 data: Tribal districts report high levels of malnutrition and poverty.*
  - **Inequitable Development**: Benefits of liberalization and economic growth have bypassed tribal belts, creating a **"development vacuum"**.
- **Political-Institutional Causes**
  - **Weak Governance and State Absence**: In LWE-prone areas, access to public services (health, education, justice) is minimal or absent.
    - **Example:** In many villages of Bastar, there was no panchayat or police station for decades.
  - **Corruption and Exploitation**: Forest officials, police, and local contractors often exploit tribals. Disillusionment with the state creates space for Maoist ideology.
  - **Lack of Political Representation**: Tribals and Dalits are underrepresented in decision-making at higher levels.
- **Historical and Ideological Causes**
  - **Legacy of Feudalism**: In states like Bihar and Telangana (erstwhile Andhra), oppressive feudal structures led to mass mobilization of landless peasants.
  - **Ideological Indoctrination**: Maoist ideology offers a sense of purpose and empowerment to the marginalized by framing the state as exploitative.
  - **Failure of Land Reforms**: The non-implementation of land ceiling acts and land redistribution in several states widened the inequality gap.
- **Geographical and Administrative Causes**
  - **Difficult Terrain and Forest Cover**: Dense forests provide safe havens for guerrilla warfare, especially in Bastar, Gadchiroli, and Dandakaranya regions.
  - **Border Districts and Administrative Overlaps**: Maoists exploit inter-state borders and jurisdictional ambiguities (e.g., Chhattisgarh-Odisha border) to avoid crackdowns.
- **Alienation of Tribal Communities**
  - **Violation of Constitutional Provisions**:

    - Improper implementation of **Fifth Schedule**, **PESA Act (1996)**, and **Forest Rights Act (2006)**.
    - Denial of **Community Forest Rights** to many eligible tribal groups.
  - **Cultural Alienation**: Erosion of traditional tribal governance and disregard for their customs and languages creates alienation.
- **Security Gaps**
  - **Under-policing and Poor Infrastructure**: Lack of road connectivity, telecom networks, and police presence gives Maoists operational freedom.
  - **Intelligence and Coordination Failures**: Inter-state coordination among security forces is often poor, aiding the movement's mobility.



Challenges in Countering Left-Wing Extremism (LWE)

- **Terrain and Geography**
  - **Difficult Topography**: LWE-affected areas such as **Bastar (Chhattisgarh)** and **Gadchiroli (Maharashtra)** are covered with dense forests and hilly terrain, facilitating guerrilla warfare and ambushes.
  - **Poor Connectivity**: Lack of roads, telecom, and internet hampers both development and counter-insurgency operations.
- **Inter-State Jurisdictional Issues**
  - **Cross-border Safe Havens**: Maoists operate across tri-junctions (e.g., Chhattisgarh-Odisha-Andhra), exploiting gaps in coordination between state police forces.
  - **Lack of Unified Intelligence Grid**: Fragmented intelligence architecture delays proactive action.
- **Weak Governance and State Presence**
  - **Governance Vacuum**: In many tribal areas, **basic services like schools, healthcare, and PDS** are absent or dysfunctional, eroding faith in the state.
  - **Poor Implementation of Development Schemes**: Funds under schemes like **Aspirational Districts Programme** often remain underutilized or poorly targeted.
- **Socio-Economic Grievances**
  - **Land Alienation**: Displacement due to mining, dams, and industrial projects without proper compensation continues to fuel discontent (e.g., Hasdeo Arand case).
  - **Delayed Forest Rights**: Poor implementation of **FRA 2006** and **PESA Act 1996** alienates tribal communities.
- **Security and Operational Limitations**
  - **Manpower Shortages**: Security forces are often under-deployed or inadequately trained in counter-insurgency warfare.
  - **Casualty-Aversion and Morale**: High casualty operations (e.g., Sukma 2021) affect morale and operational aggressiveness.
  - **Limited Use of Technology**: Until recently, surveillance drones and AI-based threat analysis were underused in forest areas.
- **Local Support and Coercion**
  - **Sympathy from Locals**: Maoists exploit socio-economic deprivation to gain ideological and logistical support.
  - **Fear Factor**: Civilians fear reprisals from Maoists if seen cooperating with state agencies.
- **Urban Network and Propaganda**
  - **Front Organizations**: Naxals use NGOs, unions, and student bodies for fundraising, legal defense, and propaganda.
  - **Urban Maoism**: Recent investigations (2023–24) revealed attempts to re-establish urban cells for ideological recruitment.
- **Rehabilitation and Surrender Policy Gaps**
  - **Lack of Uniform Policy**: Surrender and rehabilitation policies vary widely across states, reducing incentives for defectors.
  - **Stigmatization of Surrendered Cadres**: Difficulty in reintegration into society makes

surrendered Maoists vulnerable to re-recruitment.

- **Judicial and Legal Delays**
  - **Slow Trials**: Many arrested Maoist cadres remain undertrials for years without conviction.
  - **Pendency in UAPA Cases**: Cases under **Unlawful Activities Prevention Act (UAPA)** often see slow disposal rates.
- **Ideological Resilience**
  - Maoists continue to **project themselves as "protectors of tribal rights"** and defenders against capitalist exploitation.
  - Continued circulation of Maoist literature and training manuals sustains ideological recruitment, especially among youth.

Steps taken by Government to counter LWE

(**Note : all the data & facts given below are directly taken from PIB**)

To address the LWE menace comprehensively, the Government of India adopted a **National Policy and Action Plan (2015)**, built on a **multi-pronged strategy** involving:

I.Security Measures

- **Operation Green Hunt (2009–Present)**
  - Operation Green Hunt is the informal name given to the first large-scale, coordinated anti-Naxal operation **launched in 2009** by the Government of India.
  - It involved **joint offensives by Central Armed Police Forces (CRPF, COBRA, BSF)** and **state police** across LWE-affected states, particularly **Chhattisgarh, Jharkhand, Odisha, Maharashtra, and Andhra Pradesh**.
  - The operation focused on **regaining control of Maoist-dominated territories**, setting up **forward operating bases**, and cutting off **logistics and support systems** used by insurgents.
  - Though not officially acknowledged under this name, Operation Green Hunt marked a **decisive shift in state policy**—from defensive containment to **aggressive area domination**.
- **Strengthening of Forces and Infrastructure**
  - The **deployment of Central Armed Police Forces (CAPFs)** such as CRPF, along with the formation of additional **India Reserve (IR) Battalions**, has been crucial in providing sustained boots-on-ground presence in LWE-affected districts.
  - Since 2019, the government has set up **280 new security camps** and **15 Joint Task Forces**, helping in dominating remote areas that were previously Maoist strongholds.
  - Additionally, **six CRPF battalions** have been specially deployed to support state police forces in conducting long-duration area domination and search operations.
- **Fortified Police Infrastructure**
  - Recognizing the vulnerability of police outposts in LWE zones, the government launched a targeted initiative to enhance their survivability and deterrence. As a result, **612 Fortified Police Stations (FPSs)** have been constructed across 10 LWE-affected states, a tenfold increase from only 66 in 2014.
  - Under the **Special Infrastructure Scheme (SIS)**, dedicated funding has been provided for the upgradation of **State Intelligence Branches (SIBs)**, **Special Forces**, and **district-level police units**, ensuring they are equipped for jungle warfare and counter-insurgency operations.
- **Training and Modernization**
  - To build capacity among state police forces operating in high-risk areas, **Counter Insurgency and Anti-Terrorism (CIAT) Schools** have been set up. These centers offer specialized training in ambush handling, IED disposal, tactical maneuvering, and community engagement.
  - Further, the umbrella **Modernization of Police Forces** scheme has provided financial and technical assistance for procuring modern arms, surveillance devices, and protective

gear tailored to the forested terrain of LWE zones.

- **Security-Related Expenditure (SRE) Scheme**
  - The **SRE Scheme** plays a crucial role in financially supporting the operational readiness of state forces. Under this scheme, the Centre reimburses expenditure incurred by states on key counter-LWE activities, including training, logistics, ex-gratia payments for casualties, rehabilitation of surrendered cadres, and promotion of village defence committees.
  - Between **2014–15 and 2024–25**, a total of **₹3,260.37 crore** has been released, making it a backbone of the government's security financing framework in these vulnerable districts.
- **Technology and Mobility Enhancement**
  - The use of **helicopters for aerial surveillance and troop mobility** has improved the reach and response time of security forces in remote areas where ground mobility is constrained.
  - To bridge the communications gap, the government has planned to install **10,505 mobile towers** across LWE regions, with **7,768 towers already commissioned**. By **December 2025**, the target is to provide full mobile connectivity to all LWE-affected villages — enabling better security coordination and grievance redressal.
- **Choking Maoist Financing**
  - Financial networks are critical to sustaining insurgencies. Recognizing this, the **National Investigation Agency (NIA)** has activated a dedicated **financial crimes vertical** to disrupt hawala transactions, levy collections, and extortion rings operated by CPI (Maoist).
  - These measures have **significantly weakened the insurgents' financial lifeline**, limiting their ability to procure arms, recruit cadres, and sustain prolonged operations.
- **Civic Action and Media Outreach**
  - Winning the hearts and minds of tribal populations is essential for undercutting Maoist influence. Under the **Civic Action Programme (CAP)**, over **₹196.23 crore** has been allocated for security forces to engage in community welfare — such as organizing health camps, skill training, cultural programs, and school repair initiatives.
  - The **Media Plan** launched in LWE zones combats Maoist propaganda by producing **radio jingles, street plays, youth exchange programs, and documentaries** that highlight government initiatives and expose the brutality of Maoist violence.

II. Developmental Initiatives

- **Infrastructure Development**
  - **Road Connectivity**: Recognizing that lack of physical access both hinders state outreach and aids insurgents, the Government launched the **Road Requirement Plan (RRP-I)** and the **Road Connectivity Project for LWE Areas (RCPLWE)**. Under these schemes, a total of **17,589 km of roads have been sanctioned**, of which **14,618 km have already been constructed**. These roads serve the twin purpose of enabling **mobility of security forces** and facilitating **access to markets, schools, and health facilities** for isolated villages.
  - **Telecom Projects**: In parallel, mobile network expansion is being implemented in **three phases**, targeting **Aspirational Districts** and **44 worst-affected LWE districts**. With **10,505 towers planned** and **7,768 commissioned**, full saturation is expected by **December 2025**, enabling digital inclusion, real-time governance, and improved emergency response.
- **Special Central Assistance (SCA)**
  - To plug critical infrastructure and service delivery gaps in high-intensity LWE areas, the Government launched the **Special Central Assistance (SCA)** scheme in 2017.
  - This scheme provides funding for **schools, health centers, drinking water projects, solar power, and rural infrastructure**, especially in villages where such facilities are otherwise unviable under regular schemes.
  - Since inception, **₹3,563 crore** has been released, making it a vital tool in addressing developmental inequalities and state absence.
- **Financial Inclusion**

- Addressing economic marginalization, especially in tribal belts, has been a cornerstone of the anti-LWE development strategy.
- In this regard, the Government has facilitated the opening of **1,007 new bank branches**, **937 ATMs**, and **5,731 new post offices** in LWE-affected districts since April 2015.
- Additionally, **37,850 Banking Correspondents (BCs)** have been deployed in the 30 most affected districts, enabling doorstep banking and Direct Benefit Transfer (DBT), thereby cutting off Maoists from financial manipulation of cash-based welfare schemes.

- **Skill Development and Education**
  - Recognizing that **youth alienation and unemployment** are major drivers of Maoist recruitment, a thrust has been placed on skill building and education.
  - The government has established **48 Industrial Training Institutes (ITIs)** and **61 Skill Development Centres (SDCs)** to impart vocational skills relevant to local livelihoods and emerging markets.
  - In education, **178 Eklavya Model Residential Schools (EMRSs)** have been made functional, providing high-quality residential education to tribal students in LWE-affected blocks.
  - Notably, since 2019, over **1,143 tribal youth have been recruited into security forces**, providing employment and strengthening state-citizen trust.
- **Aspirational Districts Programme**
  - To ensure focused monitoring and data-driven governance, **35 LWE-affected districts** have been brought under the **Aspirational Districts Programme**, with the Ministry of Home Affairs playing a key oversight role.
  - These districts are monitored using indicators across health, education, agriculture, infrastructure, and financial inclusion, with performance-based rankings encouraging competition and innovation among district administrations.

III. Policy Framework:

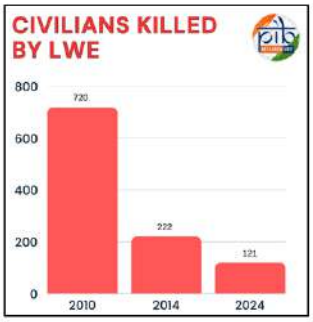
- **The government of India is committed to completely eliminate Naxalism by 31st March 2026,** since Naxalism is seen as the biggest obstacle in the development of remote areas and tribal villages, as it prevents education, healthcare, connectivity, banking, and postal services from reaching these villages.
- The government of India has adopted a **zero-tolerance approach towards left-wing extremism** and with **100% implementation of government schemes,** it seeks to fully develop the LWE-affected areas.
- **The government had laid down two rules of law to fight left wing extremism.**
  - First, to establish the rule of law in Naxalism-affected areas and completely stop illegal violent activities.
  - Second, to quickly compensate for the loss in those areas which were deprived of development due to the long Naxalite movement.
- he government of India launched the **SAMADHAN Doctrine,** it is an acronym-based strategic framework developed by the Ministry of Home Affairs for tackling LWE in a mission-mode.The doctrine integrates security, technology, accountability, and local sensitivity — shifting from a reactive to a proactive model of LWE containment.

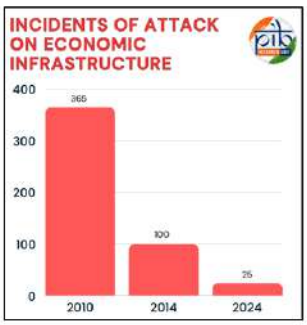
Letter	Stands for	Explanation
S	Smart leadership	Trained leadership at all operational levels; strong command structure.
A	Aggressive strategy	Proactive, offensive security operations to dismantle Maoist strongholds.
M	Motivation and training	Enhanced motivation and capacity building of police and paramilitary forces.
A	Actionable intelligence	Real-time intelligence sharing through joint

		command and control systems.
D	Dashboard-based KPIs	Monitoring progress through measurable indicators and centralized dashboards.
H	Harnessing technology	Use of drones, satellite imagery, and 4G mobile towers for surveillance and operations.
A	Action plan for each theatre	State/district-specific LWE action plans tailored to local realities.
N	No access to financing	Cutting Maoist funding via financial tracking, NIA probes, and freezing assets.

Recent Development / Trends
Data & Facts

- **According to latest update from the Home Ministry**
  - The number of districts affected by Maoism has reduced to 18 from the earlier 38.
  - "Among these, the number of **most-affected districts** has reduced to six from 12, number of **districts of concern** has also come down to six from nine, and number of other LWE-affected districts has also been reduced from 17 to six," the Ministry said in a statement.
  - **The six most-affected districts** are Bijapur, Kanker, Narayanpur, and Sukma in Chhattisgarh; West Singhbhum in Jharkhand; and Gadchiroli in Maharashtra.
  - Incidents of violence by LWE which reached its highest level of 1936 in 2010 have reduced to 374 in 2024 i.e. a reduction of 81%. The total number of deaths (civilians + security forces) has also reduced by 85% during this period from 1005 deaths in 2010 to 150 in 2024.





State-wise details of LWE perpetrated violence (number of deaths recorded) in the last 3 years are as given under

State	2022	2023	2024
Andhra Pradesh	3	3	1
Bihar	11	4	2
Chhattisgarh	246	305	267
Jharkhand	96	129	69
Kerala	0	4	0
Madhya Pradesh	16	7	11
Maharashtra	16	19	10
Odisha	16	12	6
Telangana	9	3	8
West Bengal	0	0	0
TOTAL	413	485	374

Maharashtra Special Public Security (MSPS) Bill, 2024

Context :

- With concerns over the **urban spread of Naxalite influence**, the Maharashtra government has introduced the **MSPS Bill, 2024** to address the evolving nature of Left-Wing Extremism (LWE) that allegedly uses **urban networks, frontal organizations, and safe havens** to sustain its activities. The Bill seeks to fill gaps in existing laws like the **UAPA** and **MCOCA**.

Key Features of the MSPS Bill, 2024

Objective:

- To equip the state with a legal mechanism to **identify, ban, and prosecute** individuals and organizations linked with Naxalite activities, especially in **urban settings**, through an expedited and autonomous process.

Salient Provisions:

- **Declaration of Unlawful Organizations**: The Bill empowers the state government to designate any group as "unlawful" based on its activities, without requiring central approval.

- **Defined Offences**:
  - Being a member of such an organization.
  - Raising funds or providing logistical assistance.
  - Managing or aiding in carrying out activities that disturb public order or incite fear.
  - These are **cognisable** and **non-bailable** offences.
- **Penalties**: Convictions attract **2 to 7 years of imprisonment** and **fines between ₹2 lakh to ₹5 lakh**.
- **Expedited Process**:
  - Unlike UAPA, which requires approval from the Centre and judicial tribunals, the MSPS Bill allows **District Magistrates and Police Commissioners** to sanction prosecutions.
  - An **Advisory Board** comprising former judges or qualified persons (not necessarily High Court judges) will oversee appeals against unlawful organization declarations.
- **Seizure Provisions**: The Bill permits **confiscation of property**, sealing of premises, and **eviction orders** against entities aiding banned organizations.
- **Comparison with UAPA:**
  - While the **UAPA** deals with both terrorism and unlawful activities, the **MSPS Bill broadens the scope** to include **acts affecting public order, civic administration, and inciting fear**.
  - It removes certain **judicial checks** embedded in UAPA, potentially allowing **quicker enforcement** but also raising concerns over **procedural safeguards**.

Criticism and Concerns

- **Vagueness and Overbreadth**
  - Terms like “menace to public order” or “encouraging disobedience” are **not precisely defined**, leaving room for **arbitrary interpretation and misuse**.
- **Threat to Civil Liberties**
  - Critics fear the law may be **used against dissenting voices**, including **journalists, student activists, and NGOs**, under the guise of countering urban Maoism.
  - The broad definitions may **blur the line between peaceful protest and criminal conspiracy**.
- **Diluted Judicial Oversight**
  - Unlike UAPA, where judicial tribunals led by High Court judges review bans, the MSPS Bill assigns this role to an **advisory board** that may include **non-judicial members**, undermining impartiality.
- **Potential for Abuse**
  - The **provisions for property seizure and eviction without prior hearing** or proper redressal mechanisms raise the risk of **violating natural justice**.
  - The criminalization of **associational acts**, like providing aid or space, could **discourage legitimate civic engagement**.

4 North East insurgency

Introduction

- India's northeastern region (NER) covering eight states (Arunachal Pradesh, Assam, Manipur, Meghalaya, Mizoram, Nagaland, Sikkim and Tripura) have given birth to several armed insurgencies leading to indiscriminate violence and instability.
- It is another example of development and extremism being related.It is a long-standing internal security challenge involving multiple armed groups demanding autonomy, separate statehood, or secession from India.
- Rooted in ethnic aspirations and historical grievances, it has led to violence, extortion, cross-border militancy, and disruption of governance.
- The insurgency has significantly strained security forces, impeded development, and impacted India's border management, especially with Myanmar, China, and Bangladesh.

Historical Background and Evolution of North-East Insurgency

- **Colonial Legacy and Post-Independence Integration**
  - Under British rule, most tribal areas in the North-East were classified as **Excluded and Partially Excluded Areas**, governed separately and isolated from the rest of British India. This reinforced distinct ethnic identities and governance patterns.
  - After independence, **merger of tribal kingdoms and princely states**—such as **Manipur (1949)** and **Tripura (1949)**—led to discontent among local elites, who viewed the process as imposed and politically insensitive.
  - The **Naga National Council (NNC)**, under **Angami Zapu Phizo**, rejected the merger of Naga areas into India and launched one of the earliest insurgencies, seeking a sovereign Naga homeland.
- **Rise of Ethno-Nationalist Movements (1950s–1980s)**
  - **Nagaland**: Following NNC's armed struggle, its successors like the **National Socialist Council of Nagaland (NSCN)**, and its factions like **NSCN-IM (Isak-Muivah)** and **NSCN-K (Khaplang)** continued the insurgency, demanding a **Greater Nagalim**.
  - **Mizoram**: In response to poor famine relief during the **Mautam famine (1959)**, the **Mizo National Front (MNF)** launched an armed uprising in 1966, demanding independence.
  - **Manipur**: Several groups emerged in the 1970s–80s, including:
    - **People's Liberation Army (PLA)** – established in 1978.
    - **United National Liberation Front (UNLF)** – founded in 1964.
    - **People's Revolutionary Party of Kangleipak (PREPAK)** – formed in 1977. These groups sought to restore Manipur's pre-merger sovereignty.
  - **Tripura**: The influx of Bengali refugees post-Partition triggered resentment among indigenous communities. This led to insurgent outfits like:
    - **National Liberation Front of Tripura (NLFT)**
    - **All Tripura Tiger Force (ATTF)**
  - **Assam**: The **Assam Agitation (1979–1985)** against illegal immigration culminated in the emergence of the **United Liberation Front of Asom (ULFA)** in 1979, demanding a sovereign Assam.
- **Cross-Border Linkages and Escalation (1990s–2000s)**
  - Many insurgent groups established **training camps and supply chains across international borders**, especially in **Myanmar, Bangladesh, Bhutan, and China**.
  - Regional alliances like the **United National Liberation Front of Western South East Asia (UNLFW)** were formed to consolidate resources and operations.
  - There were persistent allegations of **external support from Pakistan's ISI** and **Chinese intelligence agencies**, adding a **geopolitical dimension** to these insurgencies.
- **Decline of Violence and Peace Initiatives (2010s–present)**
  - Several successful peace accords were signed, including:

- **Mizo Peace Accord (1986)** – brought MNF into mainstream politics.
- **Bodo Accords (1993, 2003, and 2020)** – led to creation of the Bodoland Territorial Region (BTR).
- **Bru-Reang Agreement (2020)** and **Tripura insurgent group surrenders** further reduced armed militancy.

- Ceasefire agreements with groups like **NSCN-IM**, and peace talks with **ULFA (Pro-talk faction)** have helped bring relative calm to the region.
- Government initiatives like the **Act East Policy**, infrastructure expansion, and rehabilitation packages for surrendered militants have aided in de-escalation.

The statewise Insurgent Group in North-East

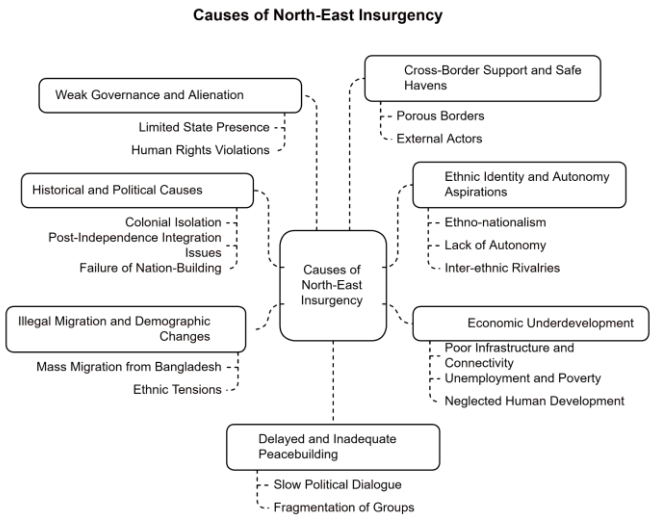
State	Insurgent Group	Main Objective	Current Status
Nagaland	National Socialist Council of Nagaland – Isak-Muivah (NSCN-IM)	Creation of **Greater Nagalim** (integrating Naga-inhabited areas)	Under ceasefire; in **peace talks**
	National Socialist Council of Nagaland – Khaplang (NSCN-K)	Same as above; split faction	Weakened; some leaders surrendered
Manipur	People's Liberation Army (PLA)	Secession; **independent Manipur**	Active; banned under UAPA
	United National Liberation Front (UNLF)	Independent socialist Manipur	Active; some factions in peace talks
	People's Revolutionary Party of Kangleipak (PREPAK)	Independent Manipur	Active; listed as terrorist organization
Assam	United Liberation Front of Asom (ULFA)	Sovereign Assam	Split: **Pro-talk faction in dialogue**, Paresh Baruah faction still active
	National Democratic Front of Bodoland (NDFB)	Separate Bodoland state	Disbanded post **2020 Bodo Accord**
Tripura	National Liberation Front of Tripura (NLFT)	Independent Tripura for tribal communities	Most factions **surrendered or inactive**
	All Tripura Tiger Force (ATTF)	Protect tribal rights, anti-migrant	Inactive; members surrendered
Meghalaya	Hynniewtrep National Liberation Council (HNLC)	Separate Hynniewtrep state for Khasis	Revived activity; currently in peace talks
	Garo National Liberation Army (GNLA)	Greater Garo Land	Declared banned; largely neutralized

Mizoram	Mizo National Front (MNF) (historical)	Independence from India	Signed **Mizo Accord (1986)**; now a political party
Arunachal Pradesh	National Socialist Council of Nagaland (NSCN factions operating in Tirap, Changlang)	Naga integration	Active; cross-border movement from Nagaland
Across States	United National Liberation Front of Western South East Asia (UNLFW)	Coalition of multiple NE groups (e.g., ULFA, NSCN-K, PLA, etc.)	Limited activity post multiple surrenders

Causes of North-East Insurgency

- **Historical and Political Causes**
  - **Colonial Isolation**: The British governed the region under **Excluded and Partially Excluded Areas**, isolating it from the Indian mainstream and fostering distinct ethnic identities.
  - **Post-Independence Integration Issues**: Hasty or contested mergers (e.g., Manipur, Tripura, and Naga Hills) without local consensus created lasting political resentment.
  - **Failure of Nation-Building**: Inadequate political representation and perceived **neglect by mainland India** fostered alienation and resistance.
- **Ethnic Identity and Autonomy Aspirations**
  - **Ethno-nationalism**: Demands for self-determination or secession by tribes like the Nagas, Mizos, Bodos, and Kukis have driven insurgencies.
  - **Lack of Autonomy**: Inadequate implementation of **Sixth Schedule provisions** and denial of autonomous councils fueled demands for separate states or regions (e.g., Bodoland, Garoland).
  - **Inter-ethnic Rivalries**: Conflicts between groups (e.g., Naga-Kuki, Bodo-Muslim) have further complicated the situation.
- **Economic Underdevelopment**
  - **Poor Infrastructure and Connectivity**: The region remains economically backward due to limited road, rail, and digital connectivity.
  - **Unemployment and Poverty**: Lack of jobs, industries, and skill development leads to youth being lured by insurgent groups.
  - **Neglected Human Development**: Low HDI indicators in health and education fuel frustration among marginalized tribal communities.
- **Illegal Migration and Demographic Changes**
  - **Mass Migration from Bangladesh** (especially into Assam and Tripura) has led to fears of demographic marginalization among indigenous groups.
  - **Ethnic Tensions**: Indigenous groups view migrants as threats to land, culture, and political power — leading to movements like the **Assam Agitation (1979–85)**.
- **Weak Governance and Alienation**
  - **Limited State Presence**: Many insurgency-affected areas lack basic public services, administrative outreach, and policing.
  - **Human Rights Violations**: Misuse of laws like **AFSPA (Armed Forces Special Powers Act)** has alienated civilians and strengthened insurgent narratives.
- **Cross-Border Support and Safe Havens**
  - **Porous Borders** with **Myanmar, Bangladesh, Bhutan**, and **China** facilitate arms smuggling, training camps, and safe havens for insurgent groups.
  - **External Actors**: Agencies like **Pakistan's ISI** and alleged support from **Chinese intelligence** have historically supplied funds and arms to NE insurgents.
- **Delayed and Inadequate Peacebuilding**
  - **Slow Political Dialogue**: Long delays in peace talks (e.g., with NSCN-IM) and failure to implement earlier accords (like the Assam Accord) have eroded trust.

- **Fragmentation of Groups**: Splinter factions emerge even after peace agreements, prolonging instability.



Steps taken by government to counter North East Insurgency

I. Security Measures

- **Strengthening Counter-Insurgency Forces**
  - Deployment of **Assam Rifles**, **CAPFs** (like CRPF), and state police in insurgency-prone districts.
  - Creation of **special forces** like **Counter-Insurgency and Jungle Warfare School (CIJWS)** in Mizoram for training in guerrilla warfare.
- **Suspension of Operations Agreements (SoO)**
  - Temporary ceasefire agreements signed with multiple insurgent groups (e.g., Kuki groups in Manipur, NSCN factions in Nagaland) to create space for dialogue.
- **Intelligence and Surveillance Enhancement**
  - Modernization of state police forces and establishment of **intelligence coordination centres**.
  - Use of **UAVs and drone surveillance** in border areas (e.g., in Arunachal, Nagaland, and Manipur).
- **Armed Forces (Special Powers) Act, 1958 (AFSPA):**
  - AFSPA grants special powers to the armed forces in "disturbed areas" to conduct operations, arrest suspects, and use force if necessary.
  - Applied in parts of Assam, Nagaland, Manipur, and Arunachal Pradesh to counter insurgent activities.
  - Example: AFSPA has been used in Nagaland to combat NSCN factions, though its prolonged use has sparked debates over human rights concerns.
- **Counter-Insurgency Operations:**
  - Targeted operations to neutralize insurgent groups, such as **Operation All Out** in Manipur and Assam against ULFA and other groups.
  - Joint operations with state police to conduct search-and-destroy missions in remote and forested areas.
- **Use of Technology:**
  - Deployment of drones, Unmanned Aerial Vehicles (UAVs), and satellite imagery for real-time surveillance in remote areas.
  - Cyber monitoring to track online extremist propaganda and recruitment networks.
  - Example: Use of drones in Manipur to monitor insurgent movements in hilly terrains.

II. Political and Peacebuilding Initiatives

- Recently a **Memorandum of Settlement** was signed, in the presence of Union Home Minister, **between the Government of India, Government of Tripura and National Liberation Front of Tripura (NLFT) and All Tripura Tiger Force (ATTF),** in New Delhi, today. The Agreement is a significant milestone to fulfil government vision of a peaceful, prosperous and insurgency-free Northeast. C
  - **Other Important agreement as follows :**

Accord	Year	Outcome
Mizo Peace Accord	1986	Ended MNF insurgency; Mizoram became a full-fledged state
Bodo Peace Accords	1993, 2003, 2020	Led to creation and expansion of

		Bodoland Territorial Region (BTR)
Naga Peace Talks	2015	**Framework Agreement (2015)** signed with **NSCN-IM**, currently under negotiation on unresolved issues like flag and constitution
NLFT (Tripura) Peace Accord	2019	Brought an end to NLFT's armed rebellion
Bru-Reang Agreement	2020	Resettlement of displaced Brus from Mizoram in Tripura

III .Developmental Measures

- **Connectivity and Infrastructure**
  - **North-East Special Infrastructure Development Scheme (NESIDS)** for roads, power, health infrastructure.
  - **Bharatmala** and **PM Gati Shakti** initiatives to boost road and logistics connectivity.
  - Expansion of **rail and air connectivity** under **UDAN scheme**.
- **Economic Integration**
  - Focus on border trade and economic corridors under **Act East Policy** to link North-East with Southeast Asia.
  - **North Eastern Council (NEC)** and **DoNER Ministry** coordinating regional development projects.
- **Skill Development and Employment**
  - Establishment of **Skill Development Centres**, **ITIs**, and **Eklavya Model Residential Schools (EMRSs)**.
  - Special economic packages and incentives for private investment in the region.
- **Diplomatic and Cross-Border Cooperation**
  - **Cooperation with Myanmar** to dismantle insurgent camps (e.g., joint operations along India-Myanmar border).
  - **Bilateral coordination** with **Bhutan and Bangladesh** to prevent safe havens for groups like ULFA and NSCN-K.
  - Efforts to secure **border fencing** and improved border management systems.
- **Rehabilitation and Reintegration of Militants**
  - **Surrender and Rehabilitation Policies** offering vocational training, financial aid, and soft loans to surrendered cadres.
  - Over **9,000 insurgents** surrendered across the region between 2014–2023 (MHA data).
- **Promoting Cultural and Ethnic Reconciliation**
  - Support for **autonomous councils** (under Sixth Schedule) to recognize tribal aspirations.
  - Encouragement of **inter-community dialogues** and peacebuilding efforts at grassroots level.

Recent Developments / Trends

Data / Facts

- **According to the Union Ministry of Home Affairs (MHA) annual report for 2023-24.**
  - **Manipur accounted for 77% of violent incidents** that took place in northeastern India in 2023.
  - There were 243 violent incidents reported in the northeast in 2023, of which 187 were in Manipur.
  - The Union government released ₹247.26 crore to Manipur in 2023 to operate relief camps and rehabilitate people affected by the State's "law and order crisis."

Recent Manipur Insurgency

Context

- **Overview**: Since May 2023, Manipur has faced a resurgence of insurgency amid ethnic violence between the Meitei (majority, Imphal Valley) and Kuki-Zo (tribal, hill districts) communities, described by some as a civil war. The conflict has caused over 260 deaths, displaced 60,000 people, and led to significant property destruction.
- **Trigger**: A Manipur High Court order in April 2023, recommending Scheduled Tribe (ST) status for Meiteis, sparked protests by Kuki-Zo tribes fearing loss of privileges, escalating into violent clashes.
- **Insurgent Involvement**: Meitei groups (e.g.,

UNLF, PLA, Arambai Tenggol) and Kuki-Zo groups (e.g., KNO, KNA) have intensified the conflict through extortion, arms looting, and attacks on civilians.

Background

- **Historical Roots**:
  - Manipur's insurgency began in 1964 with the United National Liberation Front (UNLF), driven by discontent over the "forced" merger with India in 1949 and delayed statehood until 1972.
  - Ethnic diversity (Meiteis: 53% in valley; Nagas and Kukis: 43% in hills) and historical tensions, including Kuki-Naga clashes in the 1990s, have sustained insurgencies.
- **Key Insurgent Groups**:
  - **Meitei Groups**: UNLF, People's Liberation Army (PLA), Kangleipak Communist Party (KCP), and Kanglei Yawol Kanna Lup (KYKL) seek independence or greater autonomy.
  - **Kuki-Zo Groups**: Kuki National Organisation (KNO), Kuki National Army (KNA), and Zomi Revolutionary Army (ZRA) demand a separate state or territorial council.
  - **Naga Groups**: National Socialist Council of Nagaland (NSCN-IM) operates in Manipur, pushing for a Greater Nagaland.
- **Recent Escalation**:
  - The 2023 violence reignited insurgent activities, with Meitei militias (e.g., Arambai Tenggol) and Kuki groups under Suspension of Operations (SoO) agreements engaging in attacks.
  - Looting of 6,000 weapons and 600,000 rounds from state armories by October 2023, along with alleged external support from Myanmar, has intensified the conflict.
  - Insurgents exploit ethnic divides, with Meitei groups enforcing moral codes (e.g., bans on Hindi media) and Kuki groups demanding a separate administration.

Government Response

<u>1.Security Measures</u>

- **Deployment of Forces**:
  - **Army and Paramilitary**: Since May 2023, the Indian Army, Assam Rifles, Central Reserve Police Force (CRPF), and Border Security Force (BSF) have been deployed extensively. Over 5,000 additional paramilitary personnel (50 companies) were sent in November 2024 to address escalating violence.
  - **Operations**: Joint operations in districts like Churachandpur, Thoubal, Bishnupur, Kakching, Senapati, and Imphal East, using drone detection systems (e.g., Jiribam operations in September 2024).
  - **Rescue and Containment**: Security forces rescued 9,000 civilians in May 2023, securing areas like Imphal-Churachandpur Road.
- **Armed Forces (Special Powers) Act, 1958 (AFSPA)**:
  - Reimposed in six police station areas, including Jiribam, in November 2024 due to renewed violence, granting enhanced powers to security forces.
  - Partially lifted in March 2023 in some areas but reinstated to address the security situation.
- **Border Security**:
  - Fencing of the India-Myanmar border (30 km completed of 1,500 km planned) to curb arms inflow and insurgent movement.
  - Nullification of the Free Movement Regime with Myanmar to restrict cross-border insurgent logistics.
- **Arrests and Neutralization**:
  - Over 350 insurgents, militants, and extortionists arrested since President's Rule in February 2025, targeting both Meitei and Kuki groups.
  - **Example:** Indian Army and Assam Police apprehended an NSCN-IM cadre in Tinsukia with weapons in September 2024.
- **Replacement of Assam Rifles**:
  - CRPF deployed in Kuki-dominated areas, replacing Assam Rifles due to perceptions of bias, with two CRPF battalions deployed by September 2024.
- **Countering Arms Looting**:
  - Enhanced security at state armories after 6,000 weapons were looted in 2023, with recovery efforts through combing operations.
- **Curfews and Internet Shutdowns**:

- Curfews imposed in Imphal, Churachandpur, and other districts, with internet services suspended to prevent misinformation and insurgent coordination.

2. Other Measures

- **Dialogue Initiatives**:
  - The Centre has initiated talks with insurgent groups, including ULFA (Independent), and facilitated dialogue between Kuki and Meitei communities.
  - Tripartite SoO agreements with 25 Kuki groups since 2008, though Meitei groups like UNLF remain outside peace talks.
- **President's Rule**:
  - Imposed in February 2025 to directly manage the state's affairs, enabling stronger central intervention to restore law and order.
- **Developmental Efforts**:
  - Investments in infrastructure and rehabilitation programs for surrendered insurgents to address root causes like unemployment and poverty.

Way Forward

- **Disarmament and Law Enforcement**:
  - Prioritize recovery of looted weapons and disarm both Meitei and Kuki militias to prevent further violence.
  - Prosecute vigilante groups like Arambai Tenggol and Meitei Leepun for alleged crimes, including gender-based violence, to restore trust.
- **Strengthen Border Security**:
  - Accelerate fencing of the India-Myanmar border and enhance intelligence-sharing with Myanmar to curb external support for insurgents.
- **Inclusive Dialogue**:
  - Establish a peace committee with representatives from Meitei, Kuki, and Naga communities to address conflicting demands (e.g., ST status, separate administration).
  - Engage Meitei groups like UNLF in peace talks, building on the 2023 agreement with one faction.
- **Good Governance**:
  - Ensure transparent fund allocation for hill and valley development to reduce ethnic disparities and grievances.
  - Strengthen local police and judicial systems to address complaints, especially from tribal communities, and reduce impunity.
- **Community Engagement**:
  - Expand civic action programs by security forces to build trust, similar to Assam Rifles' initiatives in other North East states.
  - Counter insurgent propaganda through education and awareness campaigns targeting youth.
- **Address Root Causes**:
  - Invest in equitable development (e.g., schools, hospitals, jobs) in hill districts to reduce alienation among Kuki-Zo tribes.
  - Resolve the ST status issue through a balanced approach, possibly revisiting the Manipur High Court's order under Supreme Court guidance.
- **Regional Stability**:
  - Prevent spillover of Manipur's conflict into neighboring states by strengthening regional coordination under the North East Council.

Impact of Bangladesh's Political Shift on North-East India's Geopolitics and Security

Context (In Brief)

- Following **Sheikh Hasina's resignation in 2024** amid a student-led uprising over reservation policies, a new government led by **Muhammad Yunus** has taken charge in Bangladesh. This **unexpected political transition** signals a possible shift in Dhaka's foreign policy orientation, with **direct implications for India's North-East**, which shares deep security, economic, and connectivity ties with Bangladesh.

Background: Bangladesh–North East India Relationship

- **Geographical Dependence**: India's North-East shares a **1,879 km border** with Bangladesh. States like **Tripura, Assam, and Meghalaya** depend on **Bangladesh's ports (e.g., Chittagong)** for maritime access and reduced logistic costs.
- **Connectivity Projects**: Projects like the

Agartala–Akhaura rail link, **Maitri Bridge**, and **Bangladesh–India coastal shipping** are key to North-East's integration with Southeast Asia.

- **Trade & Economy**: Trade volumes are growing—Bangladesh is a key importer of North-East's agricultural produce; the **Palatana power plant in Tripura** supplies electricity to Bangladesh.
- **Security Cooperation under Hasina**: Sheikh Hasina's tenure saw the **extradition of insurgent leaders (e.g., ULFA)**, enforcement of the **Land Boundary Agreement (2015)**, and clampdowns on **insurgent camps** in Bangladesh.

Impact of Political Shift on North-East India

- **Security Setbacks**
  - **Policy uncertainty** may weaken border intelligence sharing and counter-insurgency collaboration.
  - Possibility of **resurgence of insurgent safe havens** inside Bangladesh if the new regime deprioritized security ties.
  - The **2013 Extradition Treaty** and operational cooperation could face implementation challenges.
- **Economic and Infrastructure Disruption**
  - Key projects like **Agartala–Akhaura rail link**, **Tripura–Bangladesh energy projects**, and **transshipment routes** via Bangladesh may face delays.
  - **Rise in tariffs**, **non-tariff barriers**, and **restricted access** to ports like Chittagong could **isolate the region further**.
- **Border Management & Migration**
  - Increased **risk of porous borders**, arms and narcotics smuggling, and informal migration.
  - Could **amplify internal tensions** in Assam and Tripura over demographic shifts.
- **Geopolitical Repercussions**
  - Bangladesh's foreign policy realignment may **tilt toward China or other regional blocs**, weakening India's eastern influence.
  - May strain the **Act East Policy** linkages, as Bangladesh acts as a bridge to Southeast Asia.

Strategic Alternatives for North-East India

- **Connectivity**
  - Expedite **Kaladan Multi-Modal Transit Project** (India–Myanmar–Sittwe Port).
  - Accelerate completion of the **India–Myanmar–Thailand Trilateral Highway**.
  - Increase engagement with **port infrastructure in Myanmar (Sittwe, Dawei)**.
- **Trade and Investment**
  - Deepen ties with **BIMSTEC nations** and **ASEAN economies** (Thailand, Vietnam).
  - **Leverage Japanese investments** for industrial corridors and infrastructure.
  - Promote **North-East as a hub** under the Act East Policy.
- **Security Measures**
  - Enhance **border fencing**, **drone surveillance**, and **cross-border patrols**.
  - Innovate counter-insurgency frameworks like **AFSPA + civil intelligence cooperation**.
  - Build **regional information-sharing platforms** for intelligence and anti-smuggling efforts.

Way Forward

- **Diplomatic Engagement**: India must engage the new Bangladeshi leadership early to safeguard shared gains.
- **Regional Rebalancing**: Diversify economic and strategic dependencies to avoid over-reliance on a single partner.
- **Boost Internal Resilience**: Prioritize infrastructure, border security, and internal governance in the North-East to minimize external vulnerabilities.

Value Addition

Keywords : Left-Wing Extremism, Maoist Insurgency, Red Corridor, Tribal Displacement, Forest Rights, Governance Deficit, Developmental Alienation, Ideological Radicalization, Counter-

Insurgency, Internal Security, Urban Extremism, Cyber Surveillance, Strategic Deterrence, Guerrilla Warfare , Ethno-Nationalism, Cross-Border Insurgency, Political Autonomy, Participatory Development, Rehabilitation Policy, Act East Policy.

Mains Question for Practice :

Q1."Extremism is both a cause and a consequence of underdevelopment." Analyze with reference to Left-Wing Extremism (LWE) in India.

Q2. Evaluate the impact of the Government's SAMADHAN doctrine in countering LWE. What more needs to be done?

Q3. Examine the historical and political causes behind the insurgencies in North-East India.

Q4.Critically examine the Maharashtra Special Public Security Bill, 2024. Does it strike a balance between security and civil liberties?

Q5.Discuss the implications of political changes in Bangladesh for the security and geopolitics of North-East India.

In news

- **Breakthrough in Anti-Naxal Operations**
  - Recently, the killing of top Maoist leader Basavaraju in Chhattisgarh's Narayanpur marked a significant blow to Naxalism, with security forces intensifying efforts to dismantle insurgent networks while promoting state-building in tribal areas.
- **Government's Resolve to End Naxalism**
  - Recently, Union Home Minister Amit Shah announced a relentless strategy to eradicate Naxalism by March 2026, reducing affected districts from 12 to 6 through aggressive operations and development initiatives.
- **PM Warns Against Urban Naxalism**
  - Recently, PM Narendra Modi emphasized tackling "Urban Naxalism" as a growing threat, urging citizens to counter forces exploiting economic grievances to destabilize India's progress.
- **MHA's Roadmap to Eliminate LWE**
  - Recently, the Ministry of Home Affairs released a booklet detailing India's comprehensive plan to eliminate Left Wing Extremism by March 2026, combining security crackdowns with infrastructure development in affected regions.
- **Chhattisgarh's Dual Approach to Insurgency**
  - Recently, intensified anti-Naxal operations in Chhattisgarh led to 131 Naxalites killed this year, alongside efforts to integrate tribal communities through schools, healthcare, and economic opportunities to curb insurgency.
- **Progress in Peace Talks with Northeast Insurgents**
  - Recently, Union Home Minister Amit Shah urged remaining Northeast insurgent groups to surrender, noting that over 10,500 militants have laid down arms since 2014, with 12 peace accords signed between 2019 and 2024 to foster development and stability.
- **Economic Push to Curb Insurgency**
  - Recently, PM Narendra Modi highlighted a ₹1.55 trillion investment by major companies in the Northeast, aiming to transform the region from a hub of "bombs, guns, and blockades" into an economic hotspot, reducing insurgency through development.
- **Tensions Over Bangladesh's Remarks**
  - Recently, a retired Bangladeshi general and aide to Muhammad Yunus provoked controversy by suggesting Dhaka ally with China to occupy Northeast India if India attacks Pakistan, prompting India to restrict Bangladeshi goods' transit through the region

Case Studies

Case studies:

- **Parikrma Humanity Foundation: Urban Education and Empowerment**

- Operating in Bangalore, the Parikrma Humanity Foundation focuses on providing comprehensive education to children from underprivileged backgrounds. By addressing educational inequities and offering holistic development programs, the foundation works to break the cycle of poverty and reduce susceptibility to extremist influences.

- **Anandwan model:**
  - Anandwan's model addresses some underlying issues such as poverty, inequality, and lack of opportunities that contribute to the appeal of extremist ideologies. By providing a blueprint for inclusive development, vocational training, and community building, Anandwan showcases an alternative approach to addressing socio-economic challenges that are often associated with regions affected by Naxalism.
- **Maharashtra's Gadchiroli Model:**
  - The Gadchiroli district in Maharashtra adopted a comprehensive approach, involving the police, administration, and civil society. They focused on infrastructure development, healthcare, education, and skill-building initiatives. This integrated approach aimed to address socio-economic disparities and reduce the appeal of extremism.
- **Chhattisgarh's Amcho Bastar, Amcho Police Campaign:**
  - The Chhattisgarh Police initiated the "Amcho Bastar, Amcho Police" campaign, focusing on building trust with local communities. They organized community outreach programs, set up police-public interaction forums, and implemented development projects. This approach aimed to address grievances and reduce support for Naxalites.
- **Andhra Pradesh's Greyhounds Operation:**
  - The Andhra Pradesh Police's Greyhounds is a special force formed to combat left-wing extremism. They implemented a successful strategy combining intelligence gathering, targeted operations, and community engagement. This approach significantly weakened the Maoist insurgency in the state.
- **Salwa Judum: A Controversial Counter-Extremism Approach**
  - Initiated in Chhattisgarh, Salwa Judum was a state-supported militia aimed at combating Naxalite insurgency. While it mobilized local populations against extremism, the movement faced criticism for human rights violations and was eventually deemed unconstitutional by the Supreme Court. This case underscores the complexities and potential pitfalls of community-based counter-extremism initiatives.

Acronym

CRISIS (*CRISIS helps frame extremism as a result of chronic development neglect and governance breakdowns.***)**

- **C – Corruption**
- **R – Regional Disparities**
- **I – Illiteracy**
- **S– Social Marginalization**
- **I – Infrastructure Deficit**
- **S – Security Lapses**

THREATS

(Use for showing how underdevelopment leads to extremism and related security issues.)

- **T – Tribal Alienation**
- **H – Hostile Terrain & Poor Infrastructure**
- **R – Radical Ideologies Flourishing in Vacuum**
- **E – Economic Deprivation**
- **A – Administrative Inefficiency**
- **T – Technology Misuse by Extremists**
- **S – Security Apparatus Weakness**

PREVENT

(Use this for a solution-oriented structure.)

- **P – Participatory Governance**
- **R – Rehabilitation of Affected Regions**
- **E – Education and Awareness**
- **V – Vocational Training & Livelihood**
- **E – Effective Policing**

- **N – National Integration Initiatives**
- **T – Technology Use for Surveillance & Delivery**

Ready- Made templates

- **3C Strategy:**
  - **Coordination** – Among intelligence, security, and civil agencies.
  - **Community Involvement** – Empowering local communities to act as stakeholders.
  - **Counter-narratives** – Challenging extremist ideologies through media, education, and influencers.
- **5R Strategy:**
  - **Recognition** – Identify hotbeds of radicalism.
  - **Rehabilitation** – Reintegration programs for former militants.
  - **Reconstruction** – Rebuilding conflict-affected regions.
  - **Resilience** – Building societal resistance to extremist ideas.
  - **Reform** – Political and socio-economic reforms to address root causes.
- **4P Strategy:**
  - **Prevention** – Early identification of radicalization signs.
  - **Protection** – Enhancing physical and cyber infrastructure.
  - **Prosecution** – Legal framework to punish acts of terror.
  - **Partnerships** – International and regional collaborations.

Ready-Made Intro & Conclusion

INTRODUCTIONS:

- **Quote-Based:**
  "Poverty is the worst form of violence." – Mahatma Gandhi.
  The persistence of extremism in LWE and North-East India stems not only from ideology but from systemic neglect, poverty, and governance gaps.
- **Data-Driven:**
  Over **90% of LWE violence** occurs in districts with poor socio-economic indicators. The correlation between developmental vacuum and extremism is too strong to ignore.
- **Thematic:**
  Extremism often thrives where the state is absent and hope is scarce. In India's Red Corridor and North-East, lack of inclusive development has bred discontent and militancy.
- **Policy Angle:**
  Despite security operations, the spread of extremism continues due to unaddressed root causes—land alienation, unemployment, and poor governance.

CONCLUSIONS:

- **Solution-Oriented:**
  Guns may silence militants, but only development can silence the cause. Empowering people through education, jobs, and rights is the real antidote to extremism.
- **Quote-Based:**
  "You can't shake hands with a clenched fist." – Indira Gandhi.
  Dialogue and development must walk hand in hand to dismantle the foundations of extremism.
- **Balanced View:**
  A synergy of security, development, and dialogue is key. Winning hearts and minds, not just battles, is essential for lasting peace.
- **Analytical:**
  Extremism is not just a law-and-order issue—it's a development failure. A state that delivers opportunity need not fear insurgency.

Causes of left wing extremism/ north east insurgency:

Heading	Subheadings
Political	• Political apathy • Corruption • Poor governance
Social	• Tribal displacement • Marginalisation • Social exclusion • Racial discrimination
Economic	• Poverty • Inequality • Capitalistic exploitation
Geographical	• Resource conflict • Isolation

2 UNIT — Role of External State and Non-state Actors in creating challenges to Internal Security.

Navigating the Syllabus: What You Need to Know

Role of External State and Non-state Actors in creating challenges to Internal Security.

- Meaning and Concept of State and Non-State Actors
- Their involvement in spreading terrorism and affecting Internal Security (State-Sponsored Terrorism)
- Steps needed to prevent such activities

UPSC Previous year Questions

Question	Nature of Question	Core Demand
The use of UAVs by adversaries across borders to ferry arms, drugs, etc., is a serious internal security threat. Comment on the measures being taken to tackle this. (2023)	Emerging Threat + Policy Measures	Comment on threats posed by UAVs and steps taken by India.
Analyse the multidimensional challenges posed by external state and non-state actors to India's internal security. Also discuss measures to combat these threats. (2021)	Analytical + Strategic	Analyse threats and suggest measures to tackle state and non-state actor challenges.
Ban on Jammat-e-Islami in J&K highlighted the role of over-ground workers (OGWs). Examine their role and suggest measures to neutralize them. (2019)	Terror Support Networks + Strategy	Examine role of OGWs and suggest counter-strategies.
Briefly describe CPEC and explain why India has distanced itself from it. (2018)	Geopolitics + National Interest	Describe CPEC and state India's objections to it.
Insurgency in North-East India persists. Analyze major reasons for its survival. (2017)	Internal Conflict + Root Causes	Analyze key reasons for continued insurgency in North-East India.
India's diverse society is not immune to radicalism from the neighborhood. Discuss with counter strategies. (2014)	Social Fabric + Regional Influence	Discuss radicalism threats and counter strategies for India.
What is 'airspace' under international civil aviation laws? Discuss implications above this space and related threats. (2014)	Airspace Sovereignty + Security	Define airspace, discuss related challenges and containment strategies.
Impact of piracy risk zone shift by IMO in Arabian Sea on India's maritime security. (2014)	Maritime Security + Risk Mapping	Discuss maritime security concerns due to piracy risk zone shift.

1 External State and Non-state Actors

Introduction

External state and non-state actors significantly influence a nation's internal security by exploiting vulnerabilities through proxy warfare, cyberattacks, terrorism, and disinformation campaigns. Their actions, ranging from state-sponsored insurgencies to transnational criminal activities, challenge national stability and sovereignty. Understanding their roles is crucial for developing effective countermeasures to safeguard internal security.

External State Actors

What is meant by external state actors ?

- **External state actors** refer to **foreign governments or their agencies** that directly or indirectly interfere in the internal affairs of another country, with the intent to **destabilize, influence, or manipulate** its political, social, economic, or security environment.
- Their involvement can take the form of **sponsoring terrorism, supporting insurgencies, facilitating cyber attacks, spreading disinformation**, or engaging in economic coercion — often under the guise of **plausible deniability or proxy warfare**.

How external state actors creates challenges to internal security of India

- **Sponsorship of Cross-Border Terrorism**
  - **Example**: Pakistan's state agencies, especially the **ISI (Inter-Services Intelligence)**, have long been accused of supporting terror groups like **Lashkar-e-Taiba (LeT)** and **Jaish-e-Mohammed (JeM)** to operate in **Jammu & Kashmir**.
  - These groups conduct **terror attacks**, **radicalization**, and **infiltration**, aimed at disturbing communal harmony and bleeding India through a "**war of a thousand cuts**".
- **Support to Insurgencies**
  - In the past, **China** and **Bangladesh (pre-2008)** have been alleged to offer **logistical support, safe havens**, or **arms supplies** to North-East insurgent groups like ULFA, NSCN, and PLA.
  - This **external sanctuary** sustains armed movements and delays peace processes in the region.
- **Cyber Attacks and Espionage**
  - State-sponsored hackers from countries like **China** have targeted Indian infrastructure including **power grids (e.g., 2020 Mumbai blackout)**, **financial systems**, and **government networks**, posing a major risk to national security and public safety.
  - Espionage rings have also been busted involving **foreign embassies and agencies** tracking Indian defence or nuclear establishments.
- **Disinformation and Psychological Warfare**
  - Foreign governments use **social media platforms** and **information operations** to spread fake news, stoke communal tensions, and discredit institutions.
  - Example: **Coordinated foreign-linked campaigns** on Article 370 abrogation, Delhi riots, or farmer protests.
- **Economic Coercion and Debt Diplomacy**
  - China's increasing economic presence in South Asia (e.g., **China-Pakistan Economic Corridor**, port investments in Sri Lanka and Bangladesh) may create **strategic encirclement** or restrict India's influence, especially in the **North-East** and coastal regions.
  - Such moves can **influence domestic policy responses** through economic pressure.
- **Narco-Terrorism and Arms Smuggling**
  - Cross-border narcotics flow from **Pakistan via Punjab** and **Myanmar via Manipur and Mizoram** is often linked to **funding terrorism** and **insurgent activity**.
  - Example: Recent seizures of arms from Pakistan drones dropping contraband in Punjab border villages.
- **Proxy Actors in Religious and Ideological Radicalization**
  - External actors often fund or ideologically support **extremist religious groups**, radicalizing youth via online sermons, foreign education networks, or donations to **front organizations**.

- Example: Saudi-linked Wahhabi influence in some madrasas; foreign-funded NGOs promoting separatist sentiments.

External Non-State Actors

What is meant by external Non-State Actors ?

- **External non-state actors** are **individuals, groups, or organizations operating outside the formal structure of any government**, but based or supported from outside India's borders, that pose threats to India's internal security.
- These include **terrorist organizations, drug cartels, arms traffickers, separatist networks, cyber criminals**, and even **foreign-funded radical religious groups**.
- Though not officially affiliated with a state, they often act with **state support or tacit approval**, making them potent instruments of **proxy warfare and internal destabilization**.

How External Non-State Actors Create Challenges to Internal Security of India

- **Terrorism and Cross-Border Attacks**
  - **Groups like Lashkar-e-Taiba (LeT), Jaish-e-Mohammed (JeM), and Indian Mujahideen (IM)** operate across borders with foreign safe havens.
  - Responsible for **high-profile terror attacks** like the 26/11 Mumbai attacks, Pulwama suicide bombing, and fidayeen strikes in Jammu & Kashmir.
  - These outfits aim to create **fear, communal unrest, and undermine national unity**.
- **Radicalization and Extremism**
  - External non-state entities use **digital platforms, foreign religious schools (madrasas), and charities** to radicalize Indian youth.
  - Influence of **Islamic State (IS)**, **Al-Qaeda in the Indian Subcontinent (AQIS)** and foreign-based Sikh extremist groups like **Sikhs for Justice (SFJ)** has led to growing online radicalization, sleeper cells, and lone-wolf threats.
- **Cyber Threats and Information Warfare**
  - **Cybercriminal syndicates and hacktivist groups**, often based abroad, target Indian institutions to steal data or disrupt critical infrastructure.
  - Example: **Pro-Khalistani cyber defacements**, or **ransomware attacks** on Indian health and banking systems.
  - Disinformation campaigns on platforms like X (formerly Twitter), YouTube, and Telegram have been traced to **foreign-funded propaganda networks**.
- **Narcotics and Arms Smuggling**
  - **Drug cartels from the Golden Crescent (Afghanistan–Pakistan–Iran)** and **Golden Triangle (Myanmar–Thailand–Laos)** smuggle heroin, opium, and synthetic drugs through **Punjab, Manipur, and Mizoram**.
  - The **proceeds from narco-trade fund insurgency and terrorism**, especially in the North-East and border regions.
  - Small arms are smuggled via sea routes and land borders, feeding both urban gangs and insurgent groups.
- **Human Trafficking and Organized Crime**
  - Non-state criminal networks are engaged in **illegal migration, trafficking of women and children**, and **forged document rackets**, especially through **Bangladesh and Nepal borders**.
  - These networks undermine internal stability and are often **interlinked with terror financing and illegal fund transfers**.
- **Support to Separatist Movements**
  - Diaspora-linked outfits like **Sikhs for Justice (SFJ)** push the **Khalistan agenda** using online platforms, funding, and international lobbying.
  - North-East insurgent groups have previously received ideological and material support from **foreign NGOs and diaspora networks** in Europe and Southeast Asia.
- **Threat to Social Cohesion and Communal Harmony**
  - By **funding controversial NGOs**, propagating **hate speeches**, or **fueling communal narratives** on global forums, non-state actors attempt to **polarize society** and delegitimize democratic institutions.

Government Response to Challenges Posed by External State and Non-State Actors

- **Legislative and Legal Frameworks**
  - **Unlawful Activities (Prevention) Act (UAPA)**:
    - Enables banning of terrorist organizations and designation of individuals as terrorists.
    - Provides a legal framework for **detaining, prosecuting, and confiscating assets** of entities linked to foreign-based terrorism.
  - **National Investigation Agency (NIA) Act**:
    - Establishes NIA as a central agency with jurisdiction to investigate **cross-border terror, narco-terrorism, fake currency, and cyber crimes** linked to foreign actors.
  - **Foreign Contribution Regulation Act (FCRA)**:
    - Regulates foreign funding to NGOs and prevents misuse for **anti-national or secessionist agendas**.
  - **Extradition Treaties and Mutual Legal Assistance Treaties (MLATs)**:
    - India has signed extradition/MLAT agreements with many countries to **facilitate handover of fugitive terrorists and financial criminals**.
- **Intelligence and Counter-Terror Operations**
  - **Strengthening Intelligence Agencies**:
    - Agencies like **R&AW**, **IB**, and **NTRO** have been upgraded with better tech and cross-border monitoring tools.
    - **Multi-Agency Centre (MAC)** facilitates **real-time intelligence sharing** across agencies and states.
  - **Counter-Radicalization Cells**:
    - MHA and NIA operate units to monitor and neutralize online radicalization by foreign jihadi and separatist networks.
  - **Anti-Infiltration and Border Security Measures**:
    - **Border Security Force (BSF)**, **Assam Rifles**, and state police work jointly to plug infiltration routes.
    - Deployment of **smart fencing, drone surveillance**, and **integrated check posts (ICPs)** along India's **Western (Pakistan)** and **Eastern (Bangladesh, Myanmar)** borders.
- **Cybersecurity and Financial Surveillance**
  - **Indian Cyber Crime Coordination Centre (I4C)**:
    - Coordinates efforts to counter cyber threats, hacking attempts, and propaganda operations.
    - Partners with CERT-In and MHA for proactive cybersecurity response.
  - **FATF Compliance and Financial Monitoring**:
    - India follows **Financial Action Task Force (FATF)** guidelines to detect and freeze terror funding through banking, hawala, and cryptocurrencies.
    - Agencies like **Enforcement Directorate (ED)** and **FIU-IND** monitor suspicious transactions and linkages to foreign terror groups.
- **Strategic and Diplomatic Initiatives**
  - **Surgical Strikes and Defensive Offence**:
    - India has adopted a more assertive posture with **surgical strikes (2016, 2019)** and border actions to signal zero tolerance for proxy terror.
  - **International Cooperation**:
    - India actively engages in **bilateral/multilateral platforms (UN, SCO, FATF, INTERPOL)** to push for international action against Pakistan-sponsored terror and cyber threats.
    - Joint working groups and **intelligence-sharing pacts** with countries like the USA, Israel, France, and Bangladesh.
  - **Neighbourhood Diplomacy**:
    - Close cooperation with **Bangladesh** (e.g., ULFA leader extradition), **Myanmar** (joint counter-insurgency ops), and **Nepal** (anti-fake currency drive) to neutralize cross-border threats.
- **Institutional and Administrative Reforms**
  - **Creation of NSG hubs and NIA branches** in vulnerable regions.
  - Establishment of **Counter-Terrorism Division in MHA**.
  - Expansion of **joint operations commands** and **task forces** for real-time response to terrorist and insurgent threats.

2 Terrorism

Introduction

- In the previous unit, we examined the **linkage between development and extremism**, exploring how socio-economic deprivation, governance deficits, and identity-based grievances give rise to various forms of extremism in India.
- While **many extremist movements have roots in underdevelopment**, terrorism in India presents a distinct challenge. It is largely **geopolitically driven** and often fueled by the **involvement of external state and non-state actors**, particularly in sensitive regions like Jammu & Kashmir and parts of the hinterland.
- As per the **Global Terrorism Index (GTI) 2025**, published by the **Institute for Economics and Peace**, India ranks **14th out of 163 countries** in terms of the impact of terrorism—underscoring the persistent threat it poses to **national security, social harmony, and economic stability**.
- In this context, it becomes imperative to study terrorism not just as a law-and-order issue but as a complex **multi-dimensional internal security challenge** within this unit.

What is Meant by Terrorism or a Terrorist Act?

- **Terrorism** refers to the **use or threat of violence**, often against civilians or non-combatants, **to instill fear and achieve political, religious, or ideological objectives**. It deliberately targets societies and institutions to undermine stability, provoke overreaction, or gain attention to a cause.
- **Standard Definition (UN-adjacent)**
  - While there is no universally accepted definition, a commonly cited working definition is:
    - "Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government or civilian population in furtherance of political or social objectives."
- **Indian Legal Definition – UAPA, 1967 (Unlawful Activities Prevention Act)**
  - Under **Section 15 of the UAPA**, a **terrorist act** is:
    - "Any act intended to threaten the unity, integrity, security, or sovereignty of India or to strike terror in the people, using bombs, firearms, or other means, causing death, injury, or damage to property."

Key Characteristics of a Terrorist Act

Feature	Explanation
Political or Ideological Motive	Unlike ordinary crimes, terrorism aims to further a cause.
Use of Fear and Violence	Terror is the main instrument, not just physical harm.
Civilians as Targets	Designed to impact public psyche and draw attention.
Symbolic Nature	Attacks often target symbols of state or culture.

History of Terrorism in India

Terrorism in India has evolved through **multiple phases**, each rooted in distinct **geographical, ideological, ethnic, or religious motivations**.

Phased Evolution of Terrorism

Period	Region / Event	Details
1980s	**Punjab – Khalistan Movement**	The demand for a separate Sikh homeland (Khalistan) led to a violent insurgency. Key events include Operation Blue Star (1984), Indira Gandhi's assassination, and the Air India bombing (1985).
Late 1980s onwards	**Jammu & Kashmir Insurgency**	Sparked by political discontent and exploited by Pakistan, terrorism escalated after 1989, leading to armed infiltration,

		radicalization, and exodus of Kashmiri Pandits.
1990s	**North-East India (ULFA, NSCN)**	Ethnic and tribal insurgent groups demanded secession or autonomy. Violence included ambushes, extortion, and bombings, often targeting security forces and civilians.
1993	**Mumbai Serial Blasts**	A coordinated terror attack by underworld-linked groups using RDX, killing 257 people. It marked the nexus between organized crime and terrorism.
1999	**IC-814 Hijacking (Kandahar)**	Indian Airlines flight was hijacked by Pakistan-based terrorists to demand the release of Jaish-e-Mohammed leader Masood Azhar. This event exposed aviation security gaps.
2001	**Attack on Indian Parliament**	A high-profile terrorist attack by Pakistan-based LeT and JeM, bringing India and Pakistan close to war (Operation Parakram).
2005	**Delhi Serial Blasts**	A series of bombings in marketplaces before Diwali, killing over 60 people. It highlighted vulnerabilities in urban public spaces.
2006	**Mumbai Local Train Blasts**	A highly coordinated attack on suburban trains killed 200+ people in 11 minutes. It was linked to Pakistan-based terror outfits and sleeper cells.
2008	**26/11 Mumbai Attacks**	Ten LeT terrorists entered via sea route, attacking hotels, a railway station, and a Jewish center, killing 166. This led to the formation of the NIA.
2016	**Pathankot Airbase Attack**	A cross-border infiltration and attack on an Indian Air Force base by Jaish-e-Mohammed operatives, indicating lapses in perimeter and intelligence security.
2019	**Pulwama Suicide Attack**	A local youth radicalized by JeM carried out a suicide bombing on a CRPF convoy, killing 40 personnel. It led to the Balakot airstrike by India.
2025	Pahalgam Terrorist Attack on Tourists	On April 22, 2025, heavily armed militants opened fire on a group of tourists in Baisaran Valley, Pahalgam, killing 26 civilians and injuring over 20. The attackers, linked to LeT and The Resistance Front, targeted unarmed civilians. India

		responded with **Operation Sindoor**, cross-border strikes, and diplomatic countermeasures.

Post-2014: Emerging Trends in Terrorism

Trend	Explanation
Lone-wolf radicalization	Youth radicalized online via global jihadist propaganda (ISIS, al-Qaeda). Several cases reported in Kerala and Tamil Nadu.
Urban sleeper cells	Indian Mujahideen (IM) and other groups use local modules to plan low-cost, high-impact attacks in metros.
Cyber & Tech-Driven Terrorism	Use of encrypted apps, cryptocurrency, and dark web for communication, fundraising, and recruitment.
Drone-based Terrorism	Arms and explosives are smuggled via drones across the Pakistan border, especially in Punjab and J&K.

Brief Overview of terrorism in Jammu & Kashmir

<u>Terrorism in Jammu & Kashmir (J&K)</u>

Introduction

- Terrorism in Jammu & Kashmir is a **prolonged internal security challenge**, primarily driven by **cross-border infiltration, religious radicalization**, and **secessionist ideology**. Unlike Left-Wing Extremism, J&K terrorism is **less rooted in underdevelopment** and **more geopolitical in nature**, with significant external state and non-state actor involvement.

Historical Background

- **1987 Elections**: Alleged rigging and political alienation led to the rise of armed militancy in the Kashmir Valley.
- **1989–90**: Onset of mass insurgency, exodus of Kashmiri Pandits, and growing influence of Pakistan-backed groups like Hizbul Mujahideen, Lashkar-e-Taiba (LeT), and Jaish-e-Mohammed (JeM).
- **Post-Kargil (1999)**: Shift in Pakistani strategy toward proxy war using terror outfits and radicalized youth.
- **Recent Years (2016–2025)**: Emergence of local terrorists (e.g., Burhan Wani), internet-driven radicalization, drone-based infiltration, and civilian targeting.

Major Terrorist Groups Operating in J&K

- Lashkar-e-Taiba (LeT)
- Jaish-e-Mohammed (JeM)
- Hizbul Mujahideen (HM)
- The Resistance Front (TRF) – a newer proxy outfit of LeT

Key Terror Attacks in J&K

- **2001**: J&K Assembly Attack (Srinagar)
- **2016**: Pathankot Airbase Attack
- **2019**: Pulwama Suicide Bombing – 40 CRPF personnel killed
- **2025**: Pahalgam Civilian Massacre – 26 civilians killed; India responded with **Operation Sindoor**

Characteristics of Terrorism in J&K

- **Cross-border infiltration** via LoC with cover fire.
- **Targeted attacks** on civilians, security forces, and infrastructure.
- Use of **IEDs, grenades, sniper rifles, and drones**.
- Radicalization via **social media and encrypted platforms**.
- Emergence of **hybrid militants** (non-listed locals acting as part-time terrorists).

Impacts of Terrorism on Internal Security of India

- **Threat to National Integration and Sovereignty**
  - **Secessionist movements** fueled by terrorist groups (e.g., in Jammu & Kashmir, North-East India) challenge the **territorial integrity** of India.

- Cross-border terrorism from Pakistan-backed groups like **Lashkar-e-Taiba** and **Jaish-e-Mohammed** undermines **sovereignty and control** over border regions.
- Khalistani propaganda funded by diaspora groups aims to **revive separatist sentiments**, particularly in Punjab.

- **Communal Polarization and Social Fragmentation**
  - Terror attacks are often **communal in nature**, aimed at provoking riots or retaliatory violence (e.g., 2006 Mumbai train blasts, 2008 Malegaon blasts).
  - Such incidents erode **inter-community trust** and contribute to **social alienation** and **radicalization**.
- **Human and Economic Loss**
  - Thousands of **civilian and security personnel deaths**: e.g., 26/11 Mumbai attacks, Pulwama attack.
  - Destruction of public infrastructure and disruption of normal life severely affect **tourism, investment, and industrial confidence** in affected areas.
  - High cost of **counter-terrorism infrastructure**, rehabilitation, and compensation increases fiscal burden.
- **Internal Displacement and Developmental Setbacks**
  - Insurgency and terrorism lead to **displacement of civilians**, especially in Left-Wing Extremism (LWE) and North-East affected areas.
  - Development projects suffer due to extortion, destruction of assets, or fear of contractor-targeted attacks.
  - **Mining, road-building, telecom connectivity**, and **education** are particularly impacted in conflict zones.
- **Strain on Intelligence and Law Enforcement Apparatus**
  - The **asymmetric nature** of terrorism requires constant upgrading of **intelligence, cyber surveillance, and inter-agency coordination**.
  - States face challenges in maintaining **preparedness and modern policing**, especially in remote or porous border areas.
- **International Image and Diplomatic Challenges**
  - Frequent terror incidents tarnish India's global image as a safe investment and tourism destination.
  - Terrorism complicates foreign policy, especially with **neighbouring states like Pakistan, China, and Bangladesh**, demanding constant diplomatic vigilance.
- **Cyber Threats and Radicalization**
  - Use of **social media, encrypted platforms, and dark web** by terror groups has complicated tracking and enforcement.
  - Online propaganda leads to **lone-wolf attacks**, particularly among youth influenced by **Islamic State or Khalistani content**.

India's Counter-Terrorism Strategy

- **Legal Framework**
  - **Unlawful Activities (Prevention) Act (UAPA), 1967**: Enables the government to ban terrorist organisations and designate individuals as terrorists, allowing extended detention and property seizure to disrupt terror networks.
  - **National Investigation Agency (NIA) Act, 2008**: Established the NIA with nationwide jurisdiction to investigate terrorism-related offences, enhancing coordination and swift prosecution.
  - **Armed Forces (Special Powers) Act (AFSPA)**: Grants special powers to armed forces in "disturbed areas" to conduct operations against terrorists and insurgents without prior legal sanction.
  - **National Security Act (NSA), 1980**: Provides preventive detention for up to 12 months in cases where individuals may threaten national security or public order.
  - **Prevention of Money Laundering Act (PMLA), 2002**: Targets terror financing by enabling the attachment of proceeds from crimes and enforcing financial transparency in compliance with FATF norms.
- **Institutional Mechanisms**
  - **National Investigation Agency (NIA)**: Acts as the apex anti-terror probe body ensuring centralised and specialised investigation into terror crimes across states and borders.

- **National Security Guard (NSG)**: Functions as a specialised commando force for counter-terror and hostage rescue operations, especially during urban terror incidents.
- **Multi-Agency Centre (MAC)**: Serves as a centralised intelligence-sharing platform that coordinates actionable inputs among different security and intelligence agencies.
- **National Intelligence Grid (NATGRID)**: Integrates databases from over 20 agencies for real-time monitoring and predictive analysis to preempt terror activities.
- **State Anti-Terrorism Squads (ATS)**: Dedicated anti-terror units functioning at the state level to investigate and act on localised terror threats and sleeper cells.

- **Operational and Tactical Measures**
  - **Operation All-Out (J&K)**: Launched to target and eliminate militants systematically through joint operations by Army, CRPF, and state police.
  - **Border Management**: Initiatives like fencing of LoC, floodlighting, and use of sensors aim to prevent cross-border infiltration and arms smuggling.
  - **Comprehensive Integrated Border Management System (CIBMS)**: A technology-driven smart fencing system using thermal imagers, radars, and drones to secure difficult terrain borders.
  - **Drone Neutralization Systems**: Developed to intercept UAVs used to drop arms and explosives, especially in Punjab and border areas.
  - **Cyber Counterterrorism Units**: Monitor social media and encrypted platforms to track digital radicalization, propaganda, and terror recruitment.
- **Diplomatic Measures**
  - **Global Terror Listings**: India successfully pushed for the UN designation of Masood Azhar (Jaish-e-Mohammed chief) as a global terrorist, limiting his global access and funding.
  - **FATF Engagement**: India has played a critical role in pushing for compliance by countries like Pakistan and actively uses FATF mechanisms to restrict terror financing.
  - **Bilateral and Multilateral Cooperation**: India has signed extradition treaties, intelligence-sharing agreements, and engages with SCO, Quad, INTERPOL, and ASEAN to bolster its global counter-terrorism posture.
  - **Highlighting Pakistan's Role in Terrorism**: India persistently raises the issue of state-sponsored terrorism in international forums like the UNGA to diplomatically isolate offending states.
- **Financial Countermeasures**
  - **Freezing of Bank Accounts**: NIA and Enforcement Directorate freeze assets and accounts of designated terrorists and front organisations.
  - **Hawala and FCRA Monitoring**: Surveillance on informal money channels and NGOs ensures that funds are not diverted to terror-related activities.
  - **Engagement with FinCEN and Egmont Group**: India uses international financial intelligence networks to trace illicit financial flows linked to terrorism.
- **Technological and Cyber Counterterrorism**
  - **Facial Recognition and Biometrics**: Used in transportation hubs and sensitive sites to identify suspects and prevent entry of wanted terrorists.
  - **Big Data and Surveillance Tools**: Tools like NATGRID and CCTNS help map criminal-terrorist linkages and assist in real-time decision-making.
  - **Monitoring of Encrypted Platforms**: Cyber agencies track suspicious activity on platforms like Telegram and WhatsApp to disrupt digital recruitment and radicalization.
- **The New Normal in Counterterrorism**
  - India has shifted from a reactive to a proactive stance, exemplified by precision strikes like **Balakot (2019)** and **Operation Sindoor (2025)**. Emerging challenges like drone warfare, digital radicalisation, and lone-wolf attacks are being tackled through integrated, tech-driven and intelligence-based approaches.
- **Developmental and Soft Measures: Winning Hearts and Minds Approach**

Hearts and Minds Approach

- **Jammu & Kashmir Focus**
  - **Prime Minister's Development Package (PMDP-2015)** worth ₹80,068 crore targets infrastructure, education, and employment generation. Projects include AIIMS, IITs, and road/tunnel networks like **Zojila** and **Z-Morh**, improving accessibility and economic activity.
  - **Mission Youth** and **UDAAN Scheme** provide employment, skilling, and startup support to valley youth—over **70,000 beneficiaries** to date—creating avenues of hope and economic independence.
  - **Sadbhavana Missions** (especially by the Army) involve schools, medical camps, and vocational training for rural and border youth to foster trust and reduce militant sympathies.
- **De-radicalization and Community Engagement**
  - **Maharashtra's 'Deradicalisation Module'** uses psychologists, family counselling, and community leaders to engage at-risk youth before they slip into extremist ideologies.
  - **Kerala Police's Counter-Radicalisation Cell** monitors online activity and intervenes with flagged individuals using social workers and religious mentors.
- **Religious and Cultural Outreach**
  - Governments support **moderate clerics**, organize **interfaith dialogues**, and promote **inclusive curricula** to counter religious extremism.
  - Community policing and initiatives like **"Apka Mitra Police"** in Uttar Pradesh and **"Janta Ka Sipahi"** in J&K bridge the psychological gap between police and minorities.
- This strategy of **development + dignity + dialogue** is essential in fragile regions where alienation, not ideology alone, drives extremism. Winning over hearts and minds is thus not a soft option, but a strategic imperative in India's counter-terrorism doctrine.

Emerging Challenges in Counter-Terrorism in India

- **Exploitation of Emerging Technologies**
  - **Challenge**: Terrorist groups are leveraging advanced technologies, including drones, artificial intelligence (AI), encrypted platforms (e.g., Telegram, TOR), and cryptocurrencies for planning, recruitment, propaganda, and financing. The 2021 Jammu Air Force base drone attack highlighted the threat of unmanned aerial systems (UAS). Cyberterrorism targeting critical infrastructure is also a growing concern.
  - **Impact**: These technologies enable anonymity and decentralized operations, complicating detection and disruption. Informal financial networks like hawala further obscure funding trails.
  - **Response**: The 2022 Delhi Declaration by the UN Security Council's Counter-Terrorism Committee emphasizes countering technology misuse. India must bolster cybersecurity, deploy anti-drone systems, and collaborate with tech firms to monitor encrypted platforms.
- **Urban Terror and Sleeper Cells**
  - **Challenge**: Urban centers like Delhi, Mumbai, and Bengaluru are increasingly targeted due to their high population density and economic significance. Sleeper cells—covert operatives embedded in society—pose a latent threat, capable of executing attacks with minimal warning, as seen in the 2011 Mumbai serial blasts. These cells often blend into urban populations, exploiting anonymity.
  - **Impact**: Urban terror disrupts economic hubs, creates public panic, and strains security resources. Sleeper cells' low visibility makes them difficult to detect until activated.
  - **Response**: Enhanced urban surveillance, including AI-driven facial recognition and CCTV networks, is critical. Strengthening community policing and intelligence-sharing between the National Investigation Agency (NIA) and local law enforcement can help identify and neutralize sleeper cells early.

- **Use of Deepfakes and AI-Generated Propaganda**
  - **Challenge**: Terrorist groups, including the Resistance Front (TRF), are using deepfake videos and AI-generated content to incite communal hatred, recruit youth, and discredit the Indian state. AI-generated images and videos glorifying terrorists or spreading misinformation amplify radicalization efforts, particularly on social media.
  - **Impact**: Deepfakes erode public trust in institutions, fuel communal tensions, and enhance terrorist propaganda's reach. Their sophisticated nature makes detection challenging for traditional monitoring systems.
  - **Response**: India needs to invest in AI-based detection tools to identify deepfakes and counter misinformation campaigns. Public awareness campaigns and partnerships with social media platforms to remove extremist content are essential. The NIA's efforts to monitor online propaganda, such as ISIS-affiliated *Voice of Hind*, must extend to AI-generated content.
- **Lone Wolf and Decentralized Attacks**
  - **Challenge**: Self-radicalized "lone wolf" attackers and small cells, often inspired by global jihadist propaganda, are increasing. The 2022 Udaipur beheading case illustrates how individuals with no formal terrorist affiliations can execute attacks.
  - **Impact**: These unpredictable attacks evade traditional intelligence networks, as perpetrators often radicalize online and act independently.
  - **Response**: AI-driven monitoring of extremist online content, coupled with community-based deradicalization programs, is vital. The NIA should prioritize tracking radicalization pathways on social media.
- **Cross-Border and Proxy Terrorism**
  - **Challenge**: Pakistan-based groups like Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM) continue to orchestrate cross-border attacks, particularly in Jammu & Kashmir. Proxy terrorism, supported by state actors, exploits porous borders and geopolitical tensions.
  - **Impact**: These attacks destabilize regions and strain security resources, as seen in the 2019 Pulwama attack.
  - **Response**: India's zero-tolerance policy, including surgical strikes and diplomatic efforts to designate terrorist groups globally (e.g., Masood Azhar's UN listing in 2019), must continue. Advanced border surveillance and international cooperation via the Financial Action Task Force (FATF) are critical.
- **Radicalization and Internal Security Threats**
  - **Challenge**: Domestic radicalization, driven by extremist ideologies (e.g., ISIS-inspired modules), communal tensions, and socio-economic disparities, is rising. Urban and marginalized communities are particularly vulnerable.
  - **Impact**: Homegrown terrorism threatens social cohesion and overwhelms law enforcement, amplifying risks in urban centers.
  - **Response**: Community engagement, counter-narratives, and socio-economic development programs are essential. The NIA's crackdowns on ISIS-inspired cells need broader support through a national Countering Violent Extremism (CVE) policy.
- **Geopolitical Shifts and Regional Instability**
  - **Challenge**: The 2021 Taliban takeover in Afghanistan has emboldened groups like Al-Qaeda and IS-Khorasan, with potential spillover into India. China's tacit support for Pakistan-based groups adds complexity.
  - **Impact**: Transnational terrorism risks increase, and geopolitical divisions hinder global counter-terrorism cooperation.
  - **Response**: India must strengthen intelligence-sharing with allies like the US, Russia, and Israel while advocating for robust UN counter-terrorism frameworks. Regional cooperation through SAARC remains crucial despite challenges.
- **Legal and Policy Gaps**
  - **Challenge**: While the Unlawful Activities (Prevention) Act (UAPA) provides a strong legal framework, gaps in implementation,

inter-agency coordination, and global consensus on defining terrorism hinder effectiveness. The stalled Comprehensive Convention on International Terrorism (CCIT) reflects these challenges.
    - **Impact**: Inconsistent enforcement and delays in prosecution weaken deterrence, while stringent laws risk alienating communities.
    - **Response**: Streamlining coordination among the NIA, Intelligence Bureau (IB), and state police, along with judicial capacity-building, is essential. India must continue pushing for the CCIT globally.

Way Forward for Counter-Terrorism in India

- **Strengthen Intelligence Integration and Inter-agency Coordination**
    - Institutionalize **real-time intelligence sharing** through full operationalization of **NATGRID**, linking state police, IB, NIA, and other stakeholders.
    - Empower **Multi-Agency Centres (MACs)** at state and district levels with trained personnel and real-time data access.
- **Reform Legal Architecture**
    - Ensure **judicial oversight and safeguards** in laws like UAPA and NSA to prevent misuse while retaining their deterrence value.
    - Expedite the long-pending **anti-terror court reforms** for faster trial and conviction in terror-related cases.
- **Technology-Driven Surveillance and Predictive Policing**
    - Use **AI, Big Data, and facial recognition** for profiling terror suspects and monitoring digital ecosystems.
    - Expand use of **CCTNS (Crime and Criminal Tracking Network System)** and link it with NATGRID, FCRA records, and customs intelligence.
- **Counter Radicalization and Online Extremism**
    - Establish **dedicated counter-radicalization cells** in all states, similar to Kerala and Maharashtra models.
    - Collaborate with social media platforms to flag, take down, and counter extremist content with credible counter-narratives.
    - Promote **digital literacy and awareness** in vulnerable regions to build societal resilience.
- **Border Security Modernization**
    - Complete **smart fencing under CIBMS** (Comprehensive Integrated Border Management System) across porous borders, especially in Punjab, J&K, and NE.
    - Improve coordination between **BSF, Assam Rifles, ITBP, and State Police** in border zones with real-time GPS tracking and drone surveillance.
- **Devolve Responsibility to States**
    - Strengthen **State ATS units** with financial, forensic, and cybercrime capabilities.
    - Promote **inter-state coordination mechanisms**, especially in corridor zones like Bihar–Jharkhand, Assam–West Bengal, and Delhi–UP.
- **Community Engagement and Inclusive Development**
    - Deepen the **"Hearts and Minds" approach** by scaling up Civic Action Programmes and Sadbhavana missions.
    - Invest in **education, skilling, financial inclusion**, and entrepreneurship in terror-prone districts (e.g., through EMRS, PMEGP, NRLM).
    - Foster **civil society and religious leaders' partnerships** to build trust and deradicalize youth.
- **International Cooperation and Diplomacy**
- Use **multilateral platforms like FATF, INTERPOL, UNCTC, SCO, and Quad** to build a global coalition against terror financing and safe havens.
- Expand **bilateral treaties** on extradition, intelligence sharing, and legal assistance—especially with neighbouring countries like Bangladesh, Myanmar, and Nepal.

Value Addition

Keywords : External State Actors, Non-State Actors, Cross-Border Terrorism, Cyber Espionage, Radicalization, Proxy Warfare, Disinformation Campaigns, Narco-Terrorism, Religious Extremism, Internal Security, Sleeper Cells, Hybrid Militants, Drone Threats, Financial Surveillance,

Counter-Radicalization, Border Management, Cybersecurity, Terror Financing, Intelligence Sharing, Community Engagement.

Mains Practice Question :

Q1.Examine how external state actors pose a threat to India's internal security through proxy warfare and cyber operations.

Q2.Discuss the role of non-state actors in destabilizing India's internal security. How do their methods differ from those of state actors?

Q3.Critically evaluate India's policy and institutional framework in countering threats posed by external non-state actors.

Q4."Terrorism in India is more geopolitical than developmental." Discuss with reference to Jammu & Kashmir and recent terror trends.

Q5.How have lone-wolf and tech-driven terrorist tactics complicated India's counter-terrorism strategy? Suggest effective countermeasures.

In News

- **China's Alleged Support to Northeast Insurgents**
  - Recently, reports surfaced alleging China's covert support to insurgent groups like ULFA-I in Northeast India, providing financial aid and sanctuaries, fueling separatist movements and posing a persistent threat to internal security.
- **Non-State Actors Fueling Kashmir Insurgency**
  - Recently, non-state actors like Lashkar-e-Taiba and its front, TRF, were implicated in the Pahalgam attack, with local militant Adil Thokar, trained in Pakistan, aiding foreign terrorists, revealing how external non-state networks exploit underdevelopment to sustain insurgency in Kashmir
- **Bangladesh's Instigation of Ethnic Tensions**
  - Recently, provocative remarks by a retired Bangladeshi general suggested aligning with China to incite unrest in Northeast India, exacerbating ethnic tensions and challenging India's internal stability.
- **Non-State Actors Fueling Insurgency**
  - Recently, non-state actors, including dubious NGOs and extremist groups like ISIS, were reported to be radicalizing youth in Northeast India via digital platforms, contributing to internal security threats.
- **Drug Trafficking Networks Destabilizing Northeast**
  - Recently, non-state actors linked to the Golden Triangle syndicate were implicated in drug trafficking through Northeast India, undermining social stability and funding insurgent activities

Acronym

INFILTRATE

Use this to cover both external threats and internal vulnerabilities:

- **I – Ideological Warfare** (Radicalization through propaganda, cyber jihadi content)
- **N – Narcotics & Drug Trade** (Funding of extremist activities)
- **F – Fake Currency Circulation** (Economic destabilization)
- **I – Illegal Migration** (Demographic imbalance, identity crises)
- **L – Linkages with Local Insurgents** (Foreign support to Naxals/terrorists)
- **T – Terrorism Sponsorship** (Cross-border terrorism, training camps)
- **R – Remote Cyber Attacks** (Disruption of critical infrastructure)
- **A – Arms Smuggling** (Enhanced firepower to local extremist groups)
- **T – Transnational Crime Syndicates** (Organized crime networks)
- **E – Espionage Activities** (Spying, information warfare)

DEFEND
Solution based

- **D – Diplomatic Engagements** (Bilateral and multilateral cooperation)
- **E – Enhanced Intelligence Sharing**
- **F – Fortified Border Management**
- **E – Effective Cyber Security Frameworks**
- **N – National Counterterrorism Strategy**
- **D – De-radicalization and Awareness Programs**

Ready-Made Intro & Conclusion

INTRODUCTIONS:

- **Quote-Based:**
  "The enemy of my enemy is my friend" — this adage often drives covert support from external actors, turning internal fault lines into national security threats.

- **Geopolitical Lens:**
  India's internal security is increasingly shaped by cross-border influences—be it state-sponsored terrorism from Pakistan or cyber warfare from anonymous non-state actors.

- **Contemporary Context:**
  From terror financing by external agencies to radicalization through digital propaganda, India faces a new wave of hybrid threats fueled by both state and non-state actors.

- **Thematic:**
  Terrorism today is no longer a local problem. External state and non-state actors exploit ethnic, religious, and political divides to destabilize India's internal security fabric.

CONCLUSIONS:

- **Balanced Perspective:**
  Countering these challenges demands a mix of robust diplomacy, counter-intelligence, cyber readiness, and international cooperation.

- **Quote-Based:**
  "Eternal vigilance is the price of liberty." – Thomas Jefferson.
  In a globalized world, India must remain ever-vigilant against those who export terror and unrest.

- **Strategic Outlook:**
- Strengthening border management, intelligence sharing, and cyber security are crucial. Equally vital is addressing domestic vulnerabilities that external actors exploit.

- **Solution-Oriented:**
  Isolating hostile states diplomatically and dismantling non-state terror networks through global cooperation must be India's twin-pronged strategy.

Internal security threats associated with state actors.

Heading	Subheadings
Political threats	• Hampers sovereignty • Proxy wars • Insurgency • Unstable governance
Social threats	• Human rights violation • Radicalisation • Terrorism support
Economic threats	• Resources exploitation • Trade war • Tourism decay
Technological threats	• Cyber insecurity /espionage • Nuclear competition • Data threats
Geographical threats	• Border tensions • Territorial expansion • Refugee crisis

3 UNIT Linkages of Organized Crime with Terrorism.

Navigating the Syllabus: What You Need to Know

Linkages of Organized Crime with Terrorism

- Meaning of the Concept of Organised Crime and Terrorism
- How Organized Crime and Terrorism affect each other
- Challenges in controlling Terrorism and Organised Crime
- Solution

UPSC Previous year Questions

Question	Nature of Question	Core Demand
Explain how narco-terrorism has emerged as a serious threat across the country. Suggest suitable measures to counter narco-terrorism. (2024)	Narco-Terrorism + Countermeasures	Explain threat of narco-terrorism and suggest countermeasures.
Discuss the types of organized crimes. Describe linkages between terrorists and organized crime at national and transnational levels. (2022)	Organized Crime + Terror Linkages	Describe types of organized crime and their terrorist linkages.
Analyse the complexity and intensity of terrorism, its causes, linkages and obnoxious nexus. Also suggest measures to eradicate terrorism. (2021)	Terrorism + Comprehensive Analysis	Analyze causes, linkages of terrorism and suggest eradication measures.
India's proximity to major opium-growing states has worsened security. Explain linkages between drug trafficking and gunrunning, money laundering, human trafficking. Suggest countermeasures. (2018)	Illicit Trade + National Security	Explain linkages between drug trade and other crimes; suggest countermeasures.
'Hot Pursuit' and 'Surgical Strikes' are used for action against terror. Discuss strategic impact of such actions. (2016)	Strategic Operations + Impact	Discuss strategic significance of hot pursuit and surgical strikes.
Terrorism is emerging as a competitive industry. Analyze. (2016)	Terrorism + Trend Analysis	Analyze how terrorism functions like an industry and its implications.

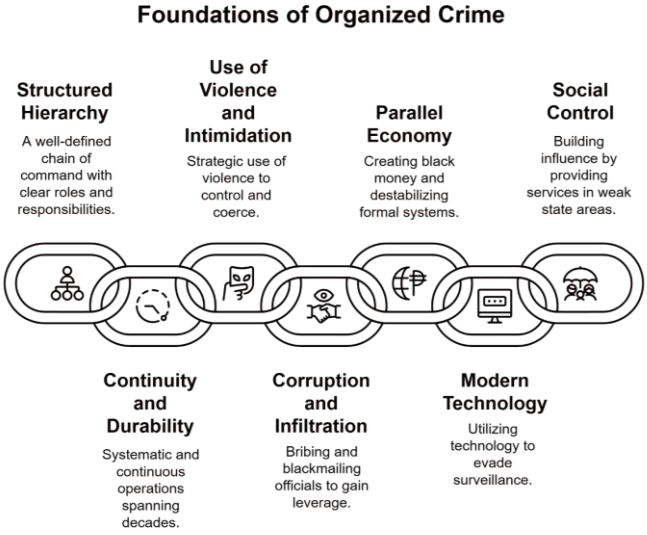
1 Organized Crime

Introduction

- **Organized crime** refers to structured groups engaging in **illegal activities on a large scale**, often using violence, corruption, and intimidation to achieve economic gain and political influence.
- In India, organized crime poses a serious threat to internal security by **funding terrorism, disrupting law and order, and infiltrating legitimate institutions**.
- Activities such as **drug trafficking, arms smuggling, human trafficking, counterfeit currency circulation**, and **underworld syndicates** have transnational linkages and often overlap with terror networks, making organized crime a complex and evolving internal security challenge.

Key Characteristics of Organized Crime

- **Structured Hierarchy**: Organized crime operates through a well-defined chain of command, often with a leader at the top and multiple operatives handling specific roles (financing, logistics, enforcement, etc.).
- **Continuity and Durability**: Unlike sporadic criminal acts, organized crime is **systematic and continuous**, often spanning decades or generations.
- **Profit-Driven Illegality**: The core aim is to **generate profit** through sustained illegal activities like drug trafficking, extortion, gambling, and smuggling.
- **Use of Violence and Intimidation**: Violence is used strategically to eliminate rivals, silence witnesses, or coerce compliance from civilians or officials.
- **Corruption and Infiltration**: Organized crime thrives on **bribing or blackmailing** law enforcement, judiciary, and political actors to escape punishment or gain leverage.
- **Global and Transnational Networks**: Many criminal syndicates operate **across borders**, dealing in narcotics, arms, and cybercrime, often coordinating with foreign entities.
- **Parallel Economy Creation**: It often leads to the generation of **black money** and **hawala networks**, which destabilize the formal financial system.
- **Use of Modern Technology**: Increasing use of **encrypted communication**, **dark web**, and **crypto transactions** to evade surveillance and law enforcement.
- **Social Control and Identity Networks**: In some regions, they build a base by providing employment, protection, or justice—especially where the state's presence is weak.



Types of Organized Crime in India

- **Drug Trafficking**
  - Involves large-scale production, transport, and sale of narcotic substances, often with international linkages and funding terror and insurgency.
  - **Example**: The **Golden Crescent** and **Golden Triangle** routes feed drugs into India. In 2023, ₹25,000 crore worth of heroin was seized off Gujarat's coast in a maritime smuggling case.
- **Arms Smuggling**
  - Illegal trade in firearms fuels militancy, organized gangs, and insurgencies, especially in border and conflict-prone regions.
  - **Example**: Sophisticated weapons from **Myanmar and China** are smuggled into India and supplied to insurgent groups like **NSCN** and **PLA** in the Northeast.
- **Human Trafficking**
  - Organized networks exploit vulnerable populations by trafficking them for forced

labor, sexual exploitation, or illegal adoption and organ trade.
    - **Example**: The **India–Nepal–Bangladesh corridor** is a hub for trafficking women and minors into metro cities like Delhi and Mumbai.
- **Cybercrime**
    - Coordinated cybercriminal operations involve online frauds, phishing, ransomware attacks, and identity theft with cross-border linkages.
    - **Example**: **Jamtara phishing gangs** in Jharkhand have been running organized scams impersonating bank officials and looting crores digitally.
- **Money Laundering**
    - Illegally earned money is routed through shell companies, hawala, or layered investments to appear legal and escape scrutiny.
    - **Example**: Hawala networks exposed by ED revealed laundering operations linked to **Dawood Ibrahim** and financing of extremist outfits.
- **Illegal Gambling and Betting**
    - Betting syndicates manipulate sports, elections, and local games to run high-stake gambling operations that generate black money.
    - **Example**: The **2013 IPL spot-fixing case** uncovered betting rings with links to Dubai-based underworld handlers.
- **Counterfeiting (Currency & Products)**
    - Fake currencies and counterfeit goods damage the economy, fund criminal activities, and pose health risks.
    - **Example**: **Fake Indian Currency Notes (FICN)** from **Pakistan** are often routed into India via **Nepal and Bangladesh**, targeting border states.

- **Environmental Crimes (e.g., Wildlife Smuggling)**
    - Criminal cartels engage in illegal trade of endangered species, forest products, and minerals, threatening biodiversity and national resources.
    - **Example**: The **rhino horn smuggling network** in Assam and **red sandalwood mafia** in Andhra Pradesh are major environmental crime syndicates.

Causes and Contributing Factors of Organized Crime

- **Economic Factors**
    - **Poverty and Inequality**
        - When people are very poor or see a big gap between the rich and the poor, they may feel desperate. If they can't find legal ways to earn money, some turn to crime. Organized crime groups offer them a way to make money, even if it's illegal.
        - **Example:** Imagine a young person in a poor neighborhood who can't afford school or find a job. A local gang might offer them quick cash to sell drugs, which feels like an easy way out of poverty.
        - **Why it matters:** Poverty creates a sense of hopelessness, and crime groups take advantage of that.
    - **Unemployment**
        - If there are no jobs, especially for young people, they may feel they have no options. Organized crime groups recruit these unemployed individuals, promising them money and a sense of purpose.
        - **Example:** In a town where factories have closed, a young adult with no job might join a smuggling ring to earn a living.
        - **Why it matters:** Without jobs, people are more likely to say "yes" to illegal work.
    - **Demand for Illicit Goods/Services**
        - People want things that are illegal, like drugs, fake designer clothes, or even human trafficking services. Organized crime groups exist to supply these things because they make a lot of money from them.
        - **Example:** If many people want to buy illegal drugs, crime groups will sell them to meet that demand, just like a store sells products people want.
        - **Why it matters:** As long as people keep wanting illegal things, crime groups will keep supplying them.
    - **Profit Motive**
        - Illegal activities like selling drugs or

weapons can make huge profits. Organized crime groups are like businesses that chase this money, even if it means breaking the law.
    - **Example:** A drug cartel might earn millions by smuggling cocaine, far more than they could earn in a regular job.
    - **Why it matters:** The chance to get rich quickly attracts people to start or join these groups.
- **Social Factors**
  - **Weak Social Structures**
    - When families, schools, or communities aren't strong, people may feel lost or unsupported. Organized crime groups act like a "family" that gives them a sense of belonging, even if it's for illegal purposes.
    - **Example:** A teenager whose parents are absent and who doesn't feel connected to school might join a gang because it feels like a supportive group.
    - **Why it matters:** Without strong communities, people are more likely to join criminal groups for support.
  - **Cultural Acceptance**
    - In some places, organized crime is seen as "normal" or even cool. Movies, music, or local traditions might make crime groups seem glamorous, so people don't see them as bad.
    - **Example:** In a city where a mafia is well-known and respected, young people might admire them and want to join.
    - **Why it matters:** If society doesn't strongly reject crime, it's easier for these groups to grow.
  - **Ethnic or Clan-Based Networks**
    - Some crime groups are built around strong family or cultural ties. These ties make the group loyal and hard to break apart because members trust each other deeply.
    - **Example:** A crime group made up of people from the same ethnic community might work together because they share language, culture, and trust.
    - **Why it matters:** These tight-knit groups are hard for police to infiltrate or stop
- **Political and Institutional Factors**
  - **Corruption**
    - When police, judges, or government officials take bribes or work with criminals, it protects crime groups. Corrupt officials might ignore illegal activities or even help the criminals.
    - **Example:** A police officer might accept money from a drug cartel to let their shipments pass through a city without being checked.
    - **Why it matters:** Corruption makes it easier for crime groups to operate without getting caught.
  - **Weak Governance**
    - If a country's government is weak or doesn't have strong control, crime groups can take over. This happens when police are underfunded, courts are slow, or laws aren't enforced.
    - **Example:** In a country with a weak government, a gang might control an entire town because the police don't have the resources to stop them.
    - **Why it matters:** Without a strong government, there's no one to fight the criminals effectively.
  - **Political Instability**
    - During wars, revolutions, or political chaos, governments are too busy to focus on crime. Crime groups take advantage of this chaos to grow stronger.
    - **Example:** During a civil war, a smuggling group might move weapons across borders because the government is distracted.
    - **Why it matters:** Chaos gives crime groups freedom to act without fear of being stopped.
  - **Legislative Gaps**
    - If laws aren't strict or up-to-date, it's easier for criminals to operate. For example, weak laws on cybercrime or money laundering let criminals get away with more.
    - **Example:** If a country doesn't have laws against certain types of online fraud,

cybercriminals can operate without being punished.
    - **Why it matters:** Outdated laws can't keep up with modern crimes, giving criminals an advantage.
- **Globalization and Technology**
  - **Global Trade and Mobility**
    - Today's world is connected by trade, travel, and shipping. Crime groups use these global networks to move illegal goods like drugs, weapons, or even people across countries.
    - **Example:** A crime group might hide drugs in a shipping container of fruit that travels from one country to another.
    - **Why it matters:** Global connections make it easier for criminals to operate across borders.
  - **Technology and Cybercrime**
    - The internet, smartphones, and encrypted apps let criminals plan and act without being caught. Cybercrime, like hacking or online scams, is a growing part of organized crime.
    - **Example:** A gang might use the dark web to sell stolen credit card numbers or plan a crime using secret messaging apps.
    - **Why it matters:** Technology gives criminals new tools and ways to hide from the police.
  - **Money Laundering**
    - Crime groups make a lot of money from illegal activities, but they need to "clean" it so it looks legal. They use global banks or businesses to hide their money.
    - Example: A crime boss might buy a restaurant and pretend their illegal money comes from selling food.
    - Why it matters: Money laundering lets criminals use their profits without getting caught.
- **Historical and Cultural Factors**
  - **Historical Precedents**
    - Some crime groups have existed for a long time, like mafias that started decades or even centuries ago. Their deep roots make them hard to stop.
    - **Example:** The Italian Mafia has been around for over a century, with traditions and networks passed down through generations.
    - **Why it matters:** Long-standing groups are well-organized and have strong connections.
  - **Cultural Norms**
    - In some places, people don't trust the government or police, so they turn to crime groups for help or protection. This makes crime groups powerful in those communities.
    - **Example:** In a village where the police are seen as corrupt, people might ask a local gang leader to settle disputes instead.
    - **Why it matters:** When crime groups are trusted more than authorities, they gain power.
- **Geographical Factors**
  - **Strategic Locations**
    - Places near borders, ports, or major trade routes are perfect for smuggling because goods and people move through them easily.
    - **Example:** A city near a border might be a hotspot for smuggling drugs because it's easy to cross into another country.
    - **Why it matters:** Location makes it easier for criminals to move illegal goods.
  - **Urbanization**
    - Big cities offer anonymity, large markets for illegal goods, and lots of people to recruit. Rural areas might be used to grow drugs or hide operations.
    - **Example:** A city gang might sell drugs in busy neighborhoods, while a rural gang grows marijuana in hidden fields.
    - **Why it matters:** Cities and rural areas both offer unique advantages for crime.
- **Individual and Psychological Factors**
  - **Greed and Ambition**
    - Some people want to be rich, powerful, or famous, and organized crime offers a fast way to get there, even if it's risky.
    - **Example:** Someone might join a crime group to become a powerful leader and live a luxurious life.

- **Why it matters:** The desire for money and status pulls people into crime.

- **Lack of Education**
  - Without education, people have fewer job options and may see crime as their only way to succeed.
  - **Example:** A dropout with no skills might join a gang because they don't qualify for legal jobs.
  - **Why it matters:** Education gives people choices, and without it, crime becomes tempting.
- **Social Exclusion**
  - People who feel left out or discriminated against may join crime groups to feel accepted or important.
  - **Example:** A minority group member facing discrimination might join a gang to feel like they belong.
  - **Why it matters:** Feeling excluded pushes people toward groups that offer a sense of community, even if it's criminal.

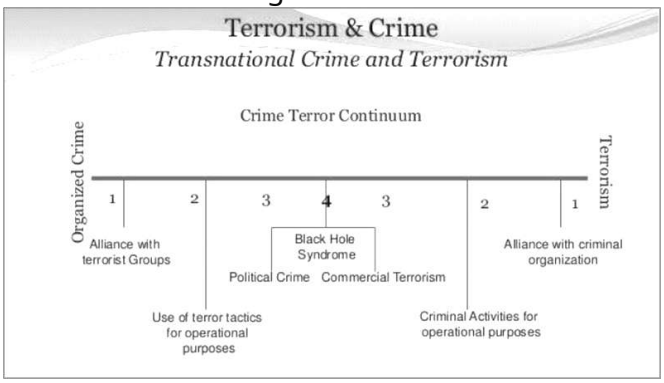
Impacts of Organized Crime

- **Undermines Rule of Law and Governance :** Criminal syndicates operate parallel power structures, often intimidating law enforcement and the judiciary. This erodes the **state's monopoly on violence**, leading to weakened state authority in certain regions.
- **Terror-Crime Nexus :** Organized crime provides funding, weapons, and logistical support to terrorist groups. For example, **underworld networks in Mumbai have been linked to Lashkar-e-Taiba** and ISI-sponsored operations, blurring lines between crime and terrorism.**(we will study more details about this in separate topic)**
- **Economic Destabilization :** Activities like **money laundering, smuggling, and counterfeit currency** damage the formal economy, create black markets, and reduce tax revenues. For instance, **Fake Indian Currency Notes (FICN)** pumped through Pakistan affect monetary stability.
- **Corruption and Institutional Decay :** Organized crime syndicates often bribe officials, thereby corrupting police, revenue, and political systems. This **hampers transparency and efficiency** in public service delivery.
- **Threat to National Security :** Smuggling of arms, infiltration through porous borders, and harboring of foreign criminals pose **direct threats to national sovereignty and border integrity**, particularly in border states like Punjab and Manipur.
- **Exploitation of Vulnerable Populations :** Human trafficking, drug trade, and illegal labor migration exploit **women, children, and the poor**, leading to violations of human rights and long-term social instability.
- **Rise in Urban Crime and Violence :** In cities like Mumbai, Delhi, and Bengaluru, organized gangs engage in extortion, contract killings, and illegal real estate deals, leading to a **climate of fear and insecurity** in urban areas.
- **Infiltration into Politics and Business :** Criminals often fund political campaigns or directly enter politics, leading to **criminalization of governance**. They also launder money through real estate and business fronts, corrupting legitimate enterprises.
- **Cross-Border Complications :** Narcotics smuggled from **Golden Crescent (Afghanistan-Pakistan-Iran)** and **Golden Triangle (Myanmar-Laos-Thailand)** enter India via porous borders, straining diplomatic and security relations with neighboring countries.

2 Nexus between Organised Crime & Terrorism

Introduction

- The nexus between organized crime and terrorism represents a grave threat to national and international security. While **organized crime is primarily profit-driven and terrorism is ideologically motivated**, both often collaborate for mutual benefit—criminal groups provide logistics, weapons, and funding, while terrorists offer protection and territory.
- **This convergence blurs the lines between criminality and extremism,** making both harder to detect and dismantle. The resulting alliance enhances the reach, resilience, and impact of both threats, posing complex challenges to law enforcement and governance.



Nature of the Nexus between Organized Crime and Terrorism

- **Operational Convergence**
  - **Terrorists use organized crime methods** (extortion, smuggling, fake documents) to fund and sustain operations.
  - **Criminal syndicates adopt terror tactics** (intimidation, bombings, killings) to dominate territories and markets.
  - ***Example*:** The **D-Company network**, originally a criminal syndicate, provided logistical support and shelter to terrorists responsible for the **1993 Mumbai blasts**.
- **Financial Convergence**
  - Terrorist groups **raise funds through criminal activities** such as narcotics trafficking, hawala networks, illegal arms trade, and human trafficking.
  - Organized crime syndicates also launder money for terrorist organizations in exchange for protection or commissions.
  - **Example: Fake Indian Currency Notes (FICN)** pumped into India by ISI-backed networks are often circulated through organized criminal routes in Nepal and Bangladesh.
- **Logistical and Infrastructure Support**
  - Terrorist groups often **outsource logistics and supply chains** (weapons, forged passports, safe houses) to existing crime networks.
  - Criminals use terror groups to **eliminate rivals or create fear**, thereby expanding their sphere of influence.
  - **Example:** Drug cartels in **Afghanistan and Pakistan** collaborate with jihadist groups for safe passage of narcotics through India.
- **Shared Networks and Safe Havens**
  - Both groups exploit **porous borders**, **corrupt law enforcement**, and **weak judicial systems** for operational ease.
  - **Common safe havens** and financial ecosystems allow both actors to thrive—especially in failed or weak states.
  - **Example:** Insurgent and smuggling groups in **North-East India and border areas like Khyber Pakhtunkhwa (Pakistan)** often use overlapping routes and contacts.
- **Ideological Camouflage**
  - Some crime groups **masquerade as ideological outfits** to gain public sympathy or evade law enforcement scrutiny.
  - Terrorist groups may **frame their criminal acts as acts of resistance** to attract recruits and donors.
  - **Example:** In some LWE (Left-Wing Extremism) zones, extortion and illegal mining are framed as revolutionary taxation.

Government steps to tackle menace of Organized crime and its Nexus with Terrorism

- **Legal Framework Strengthening**
  - **Unlawful Activities (Prevention) Act (UAPA), 1967**: Empowers the government to designate individuals and groups as terrorists and seize their assets, thereby choking financing networks linked to organized crime.

- **National Investigation Agency (NIA) Act, 2008**: Establishes NIA to investigate crimes that have inter-state and international linkages, including those arising from organized crime-terrorism nexus.
- **Prevention of Money Laundering Act (PMLA), 2002**: Tackles financial crimes, shell companies, and hawala networks used to fund terror and organized crime syndicates.
- **Foreign Contribution Regulation Act (FCRA), 2010**: Monitors NGOs and entities receiving foreign funds to prevent misuse for anti-national or terror-linked activities.

- **Institutional Mechanisms**
  - **National Investigation Agency (NIA)**: Investigates terror-financing cases, inter-state criminal syndicates, and cross-border drug/arms networks.
  - **Multi-Agency Centre (MAC)**: Facilitates real-time intelligence sharing between central and state agencies to detect and dismantle crime-terror operations.
  - **National Intelligence Grid (NATGRID)**: Integrates databases from over 20 agencies to identify suspicious financial or communication patterns used by crime syndicates and terrorists.
  - **Enforcement Directorate (ED)**: Investigates money laundering and foreign exchange violations that often fund terror modules and criminal empires.
- **Operational and Technological Interventions**
  - **Smart Fencing and Border Surveillance**: Under the Comprehensive Integrated Border Management System (CIBMS), India uses sensors, radars, and drones to check cross-border smuggling and infiltration.
  - **Cyber Counter-Terrorism Units**: Monitor dark web transactions, encrypted messaging apps, and digital currencies to trace online terror and organized crime operations.
  - **Drone Neutralization Technology**: Deployed to prevent cross-border delivery of arms and narcotics, especially along Punjab and J&K borders.
- **Financial Intelligence and Asset Seizure**
  - **Financial Intelligence Unit-India (FIU-IND)**: Tracks suspicious financial transactions to curb money laundering linked to organized crime and terrorism.
  - **Asset Forfeiture**: Through provisions under UAPA and PMLA, properties of terror financiers and criminal kingpins are seized to disrupt funding chains.
  - **Freezing of Bank Accounts and Cryptocurrency Wallets**: Government has frozen hundreds of accounts linked to terror and smuggling networks.
- **International and Bilateral Cooperation**
  - **FATF Compliance**: India is a committed member of the Financial Action Task Force (FATF) and has pushed for Pakistan's inclusion in grey/black lists for terror-financing.
  - **Interpol and Egmont Group Cooperation**: Helps trace and extradite organized crime leaders and terrorists hiding abroad.
  - **Extradition Treaties**: Signed with over 50 countries, enabling capture and deportation of wanted fugitives.
  - **Cross-Border Crackdowns**: Joint operations with countries like Nepal, Bangladesh, and Myanmar to dismantle smuggling and insurgency networks.
- **Developmental and De-Radicalization Measures**
  - **Civic Action Programme (CAP)**: Aims to build trust between security forces and local communities in areas vulnerable to crime and extremism.
  - **Skill Development and Employment**: Schemes like *UDAAN*, *Mission Youth (J&K)*, and skill centers in LWE areas reduce recruitment base for crime-terror networks.
  - **De-radicalization Initiatives**: Psychological counseling, religious engagement, and educational outreach in states like Kerala, Maharashtra, and J&K
- **Special Laws and State-Level Measures.**
  - **Maharashtra Control of Organised Crime Act (MCOCA), 1999**: A robust legal framework to prosecute organized crime syndicates and their terror links.
  - **Gujarat Control of Terrorism and Organised Crime Act (GCTOC), 2015**: Similar law empowering the state to curb syndicate-terror activities.

- **Special Task Forces (STFs)**: Set up by various states to combat high-profile criminal gangs and their terror affiliates.

Recent Development

Terror Financing

"Cutting off the funds is like severing the oxygen line of terrorism." – Financial Action Task Force (FATF)

Context :

- Recently, the **NIA hosted a two-day anti-terror conference in New Delhi**, where key issues like terror financing through organized crime, use of encrypted apps, and misuse of social media were discussed with intelligence and counter-terrorism agencies.
- Recently, **during the 4th No Money For Terror (NMFT) Conference**, India emphasized the need for global unity in combating terrorism and flagged growing concerns over the complex and cross-border nature of terror financing, especially with the rise of new digital technologies.

Sources of Terror Financing :

- **Illicit Activities**
  - **Drug Trafficking**: Terrorist groups profit from the production, smuggling, and sale of narcotics. For example, the Taliban in Afghanistan generates significant revenue from the opium and heroin trade, estimated to contribute hundreds of millions annually.
  - **Arms Smuggling**: Selling illicit weapons provides funds, as seen with groups like ISIL, which profited from black-market arms in Syria and Iraq.
  - **Human Trafficking and Smuggling**: Groups like Boko Haram and ISIL have engaged in human trafficking, including forced labor and sex trafficking, to generate income.
  - **Kidnapping for Ransom**: A major source for groups like Al-Qaeda in the Islamic Maghreb (AQIM) and Boko Haram, with ransoms yielding millions (e.g., AQIM reportedly earned over $90 million from kidnappings between 2008–2013).
  - **Extortion and Protection Rackets**: Terrorist groups like Al-Shabaab in Somalia extort local businesses and communities, often under the guise of "taxes" or "zakat."
- **Legal or Semi-Legal Sources**
  - **Charities and NGOs**: Funds are diverted from legitimate or front organizations. For instance, Hamas has historically used charitable organizations to funnel money for operations.
  - **Donations from Individuals**: Wealthy donors, particularly in regions like the Gulf, have funded groups like Al-Qaeda, often through informal networks or religious contributions (e.g., zakat).
  - **Business Ventures**: Terrorist groups invest in or operate legitimate businesses, such as real estate or import-export firms, to launder money or generate revenue. Hezbollah's global network includes such enterprises.
  - **Crowdfunding and Online Donations**: Terrorists exploit platforms like social media or cryptocurrency donations, often disguised as humanitarian causes, to raise funds anonymously.
- **State Sponsorship**
  - Some states provide direct or indirect financial support to terrorist groups to advance geopolitical goals. For example, Iran has been accused of funding Hezbollah and other proxies, providing millions in cash, weapons, and training.
  - North Korea has been linked to supporting groups through illicit trade, though evidence is less direct.
  - **Exploitation of Natural Resources**
  - **Oil and Gas**: ISIL famously controlled oil fields in Syria and Iraq, selling crude oil on black markets to earn up to $1–2 million per day at its peak (2014–2015).
  - **Mining**: Groups like the Allied Democratic Forces in the Congo exploit minerals like gold and coltan, often in collaboration with criminal networks.
  - **Timber and Wildlife**: Al-Shabaab has profited from illegal charcoal trade and ivory smuggling in East Africa.
- **Financial Systems and Technology**
  - **Money Laundering**: Terrorists use shell companies, cash couriers, or trade-based laundering to move funds. Hawala systems,

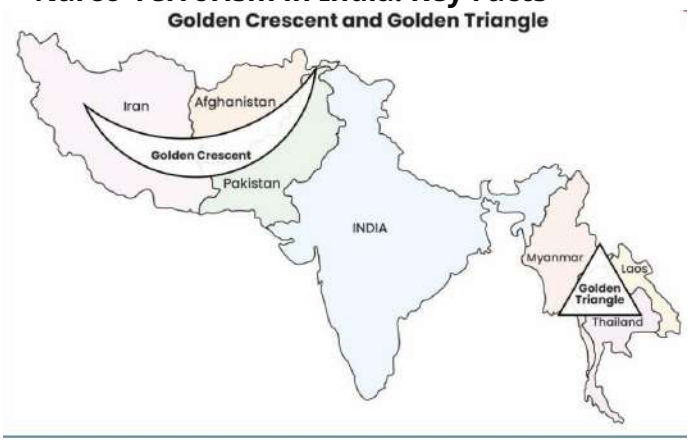
informal money transfer networks, are widely used due to their anonymity.
    - **Cryptocurrencies**: Bitcoin and other digital currencies are increasingly used for their traceability challenges, as seen in fundraising attempts by ISIL-affiliated groups.
    - **Prepaid Cards and Mobile Payments**: These provide low-risk methods to transfer small amounts across borders.
- **Local and Community Exploitation**
    - **Forced Taxation**: Groups like the Taliban and ISIL impose taxes on local populations in controlled areas, often under religious pretexts.
    - **Looting and Theft**: Terrorists fund operations through bank robberies or looting, as ISIL did during its capture of Mosul in 2014, seizing millions from banks.
- **Countermeasures in India :** *As explained above under the heading of Government steps to tackle menace of Organized crime and its Nexus with Terrorism*

Narco-Terrorism

- **Context** : The Ministry of Home Affairs (MHA) Recently informed the Lok Sabha that drugs worth over ₹11,311 crore were seized in 19 instances from seaports across the country in the past five years.
- **What is Narco-Terrorism?**
    - **Narco-terrorism** refers to the **use of drug trafficking to fund, support, or execute terrorist activities**, or the collaboration between **drug cartels and terrorist groups** to achieve their respective goals.
    - **Definition (US DEA)**: "Narcoterrorism is the participation of terrorist groups in activities of narcotics trafficking to fund their operations and gain political influence."
- **Characteristics of Narco-Terrorism**
    - **Mutual benefit alliance** between drug traffickers and terror outfits.
    - Terrorists provide **protection, weapons, and networks** in exchange for funds.
    - Enables terror groups to gain **financial autonomy**, bypassing formal state or religious donations.
    - Increases **state destabilization**, especially in border areas.
- **Global Examples**

Region	Narco-Terror Linkage
Afghanistan	Taliban funded by opium trade (80–90% of global heroin output)
Colombia	FARC rebels financed by cocaine trafficking
Mexico	Drug cartels use paramilitary tactics and terror methods

- **Narco-Terrorism in India: Key Facts**



- **Border Vulnerabilities**
    - India is between two major drug-producing regions:
        - **Golden Crescent**: Afghanistan–Pakistan–Iran
        - **Golden Triangle**: Myanmar–Laos–Thailand
    - This makes **Punjab, J&K, Northeast, and coastal areas** especially vulnerable.
- **Role in Terror Financing**
    - Drug money is used to finance **terrorist networks** like:
        - **Lashkar-e-Taiba (LeT)**
        - **Khalistani separatist groups**
        - **North-East insurgent outfits**
    - **Example**: NIA investigations (2022–24) found that **heroin smuggled into Punjab** from Pakistan was routed to fund terror sleeper cells.
- **Consequences of Narco-Terrorism**

Area	Impact

Internal Security	Narco-money sustains insurgency, buys arms, and corrodes law enforcement.
Social Fabric	Drug addiction epidemic in Punjab, NE India causes youth radicalization.
Economy	Parallel black economy undermines legitimate financial institutions.
Governance	Corruption in border forces and local administration.

Value Addition

Keywords : Narco-Terrorism, Terror Financing, Drug Trafficking, Arms Smuggling, Human Trafficking, Cybercrime, Money Laundering, Fake Currency, Underworld Syndicates, Terror-Crime Nexus, Criminalization of Politics, Cross-Border Smuggling, Hawala Networks, Financial Intelligence, Safe Havens, Parallel Economy, Dark Web, Counterfeit Currency

Mains Practice Questions :

Q1. How has globalization and modern technology transformed the nature and operations of organized crime syndicates in India?

Q2. Explain the nature of the nexus between organized crime and terrorism. Why is this convergence a major internal security challenge for India?

Q3. The distinction between ideological extremism and economic criminality is increasingly blurred." Analyze in the context of India's security landscape.

In news

- **Smuggling in India' report**
  - Recently, Directorate of Revenue Intelligence (DRI) released 'Smuggling in India' report 2023-24.highlights several alarming trends in smuggling activities across various sectors.
- **Bharatiya Nyaya Sanhita has specific provisions on organised crime**
  - Organised crime is being addressed in a comprehensive way at the national level for the first time, with its introduction in a specific section of the recently enacted Bharatiya Nyaya (Second) Sanhita (BNS), 2023. The new statute will replace the Indian Penal Code, 1860, which does not have any clauses pertaining to organised crimes, though the offence has inter-State and even international ramifications.
- **Call for urgent steps to target the organised crime.**
  - The heads of the Financial Action Task Force (FATF), Interpol, and United Nations Office on Drugs and Crime (UNODC) have called for the need to urgently step up efforts to target the huge illicit profits generated by transnational organised crime that facilitate conflicts, fund terrorism, and negatively impact vulnerable populations
- **Multi Agency Centre (MAC)**
  - Recently ,Union Home Minister Amit Shah inaugurated the revamped Multi Agency Centre (MAC), a common counter-terrorism grid under Intelligence Bureau (IB) that was conceptualised in 2001 post the Kargil war.

Acronym

FIRETRAP

(To explain how organized crime fuels terrorism)

- **F – Funding from Illicit Activities** (Drug trade, extortion, arms smuggling)
- **I – Illegal Arms Trade** (Shared supply chains for terror outfits)
- **R – Recruitment through Crime Networks**
- **E – Extortion and Kidnapping for Ransom**
- **T – Trafficking (Humans, Narcotics)**
- **R – Routes Shared Across Borders** (Smuggling and infiltration corridors)
- **A – Alliances of Convenience** (Terror-crime syndicate pacts)
- **P – Parallel Economies** (Undermining formal systems)

SHIELD *(Solutions Framework)*

- **S – Strengthen Law Enforcement Cooperation**

- **H – Harden Financial Intelligence (FIU, FATF norms)**
- **I – International Coordination (Interpol, UNODC)**
- **E – Enhanced Surveillance and Technology Use**
- **L – Legal Reforms (UAPA, MCOCA, etc.)**
- **D – Disrupt the Supply Chains (arms, drugs, funds)**

Case studies

1. 1993 Bombay Bombings
The 1993 blasts in Mumbai, carried out by Dawood Ibrahim's D-Company, exemplify the terror-crime nexus. The crime syndicate facilitated the smuggling of RDX and coordinated the attacks, showing how organized crime can provide logistics and funding for terrorism.

2. Indian Mujahideen's Criminal Links
Indian Mujahideen financed its operations through bank robberies, extortion, and counterfeit currency. These criminal acts supported terror plots and helped establish underground networks, making it difficult for authorities to trace their activities.

Ready-Made Intro-Conclusion

INTRODUCTIONS:

- **Quote-Based:**
  "Terrorists and criminals are not just enemies of the state—they are business partners in chaos." The fusion of organized crime with terrorism amplifies both lethality and resilience, posing complex challenges to internal security.
- **Conceptual:**
  Terrorism needs money; organized crime has it. When ideology meets greed, a deadly nexus is born—fueling everything from arms smuggling to narco-terrorism.
- **Contemporary Example:**
  From D-Company's links to terror funding to the use of hawala networks by jihadist outfits, the criminal-terror symbiosis in India is both real and evolving.
- **Thematic:**
  In today's security landscape, organized crime is no longer just about profit—it's a strategic enabler of terrorism, offering finance, logistics, and anonymity.

CONCLUSIONS:

- **Solution-Focused:**
  Breaking the terror-crime nexus requires synchronized intelligence, financial surveillance, and international cooperation on law enforcement.
- **Quote-Based:**
  "Follow the money" remains the most effective strategy. Disrupting the financial backbone of terror through anti-money laundering and terror funding laws is key.
- **Balanced:**
  A siloed approach won't work. India's fight against terrorism must integrate criminal justice reforms, economic surveillance, and global counter-crime frameworks.
- **Policy Angle:**
  Institutional synergy between NIA, ED, and international agencies must evolve to counter this blended threat of organized crime and terrorism.

Navigating the Syllabus: What You Need to Know

Challenges to Internal Security through Communication Networks; Role of Media and Social Networking Sites in Internal Security Challenges

- Challenges associated with Media and Social Media in Internal Security
- Steps Needed

Basics of Cyber Security

- What is Cyber Security..??
- Issues Associated with Cyber Security and their Impacts
- Steps taken and their lacunae
- Way Forward

Money-Laundering and its prevention.

- What is Money Laundering..??
- Issues Associated with Money Laundering and their Impacts
- Steps taken and their lacunae
- Way Forward

UPSC Previous year Questions

Question	Nature of Question	Core Demand
Describe the context and salient features of the Digital Personal Data Protection Act, 2023. (2024)	Legislation + Data Security	Describe context and key provisions of DPDP Act 2023.
Social media and encrypting messaging services pose a serious security challenge. What measures have been adopted? Suggest other remedies. (2024)	Tech Threats + Policy Measures	Describe existing measures and suggest remedies against encrypted platforms.
What are the internal security challenges being faced by India? Give the role of central intelligence and investigative agencies. (2023)	General Security Threats + Institutional Role	List internal threats and explain role of intelligence agencies.
What are the maritime security challenges in India? Discuss organisational, technical, procedural steps to improve it. (2022)	Maritime Security + Reforms	Describe challenges and initiatives to strengthen maritime security.
Elements of cyber security and challenges. Examine India's progress on National Cyber Security Strategy. (2022)	Cybersecurity + Policy Evaluation	List cyber security elements and assess India's cyber strategy.
Impact of cross-border cyber-attacks on internal security. Suggest defensive measures. (2021)	Cyber Attacks + National Defense	Explain impact and suggest measures against cyber intrusions.

How do technologies and globalization contribute to money laundering? Suggest national and international remedies. (2021)	Economic Crimes + Global Linkages	Explain causes and suggest steps to tackle money laundering.
Types of cybercrimes and required countermeasures. (2020)	Cyber Crimes + Preventive Strategy	List cyber crimes and state corresponding countermeasures.
What is Cyber Dome Project? How can it control internet crimes in India? (2019)	Cyber Initiative + Utility	Explain Cyber Dome and its use in crime prevention.
Discuss strengths and weaknesses of Justice B.N. Srikrishna Committee Report on data protection. (2018)	Data Governance + Critical Review	Assess Srikrishna Committee Report on personal data protection.
Potential threats of cyber-attacks and existing security framework. (2017)	Cybersecurity + Threat Mitigation	Discuss cyber threats and India's preventive framework.
Solutions to curb terrorism and major sources of terrorist funding. (2017)	Terror Funding + Solutions	Suggest anti-terror steps and identify funding sources.
Misuse of internet/social media by non-state actors. Suggest guidelines to curb it. (2016)	Tech Abuse + Policy Response	Describe misuse cases and suggest regulatory guidelines.
ISIS indoctrination via social media — what is ISIS, its mission, and how is it a threat to India? (2015)	Terror Groups + Radicalization	Explain ISIS, its aims, and threat to India via online indoctrination.
Critically evaluate the National Cyber Security Policy, 2013. Discuss implementation challenges. (2015)	Cyber Policy + Evaluation	Assess NCSP 2013 and list implementation hurdles.
Money laundering as a threat to economic sovereignty. Its significance for India and control steps. (2013)	Economic Threat + Legal Measures	Explain money laundering impact and control mechanisms in India.
What are social networking sites and what security implications do they present? (2013)	Digital Media + Threat Analysis	Explain social networks and their security challenges.
Define cyber warfare. Outline India's vulnerabilities and preparedness. (2013)	Cyber Warfare + Defense Preparedness	Explain cyber warfare and evaluate India's readiness.

1 Communication Networks, Media & Social Networking Sites and Internal Security Challenges associated with it

Introduction

The rise of digital communication networks and the widespread use of media and social networking sites have transformed how information is shared. While these platforms enable connectivity and transparency, they also pose serious challenges to internal security. From spreading misinformation and inciting violence to enabling cybercrime and terrorism, their misuse can disrupt peace and national stability. Addressing these threats requires a balanced approach that preserves freedom while ensuring security.

Differentiation between Communication Networks, Media, and Social Networking Sites:

Aspect	Communication Networks	Media	Social Networking Sites
Definition	Systems that facilitate the exchange of information via physical or digital infrastructure (e.g., internet, telephony, satellite)	Platforms for mass communication like newspapers, TV, radio, and digital news portals	Online platforms that allow users to create, share, and interact (e.g., Facebook, Twitter, Instagram)
Nature	Infrastructure-oriented (technical backbone)	Content-oriented (information disseminatio)	Interaction-oriented (user engagement)
Primary Role	Transmission of data and voice over distances	Informing, educating, and influencing public opinion	Enabling peer-to-peer and mass social interaction
Examples	Optical fibre networks, 5G, satellite networks, telecom grids	Doordarshan, The Hindu, NDTV, AIR	WhatsApp, Twitter (X), Instagram, Facebook
Governance Relevance	Backbone of Digital India, emergency communication, e-governance	Ensures freedom of press, watchdog of democracy, public accountability	Participatory governance, grievance redressal, digital campaigns
Security Implications	Vulnerable to cyber-attacks, data interception	Can spread misinformation or propaganda	Source of fake news, radicalization, cyberbullying
Regulation	TRAI, DoT, CERT-In	Press Council of India, Ministry of I&B	IT Rules, 2021; governed under IT Act, 2000

Challenges to Internal Security through Communication Networks, Media, and Social Networking Sites

Component	Key Internal Security Challenges	Examples / Data (2024–2025)
1. Communication Networks (infrastructure, internet, telecom systems)	• Cyberattacks on critical infrastructure (e.g., power grids, banking, defence) • Interception of communication by foreign intelligence • Espionage and data theft via submarine cables, satellites • Use of encrypted VPNs and dark web for illicit activities	• Over 500 cyberattacks reported in 2024 on healthcare and railway systems (CERT-In) • Mysterious Team Bangladesh and Team Insane PK targeted Indian servers (2025)

2. Traditional Media (TV, print, radio, digital news portals)	• Sensationalism and unverified crisis reporting • Communal polarization through biased narratives • Disinformation spread during elections or protests • Leak of operational details during anti-terror missions	• TV debates escalated religious tensions after 2024 Bihar incident • May 2024: Delhi school bomb threats amplified by unverified media coverage
3. Social Networking Sites (Facebook, X, WhatsApp, Telegram, Instagram)	• Spread of fake news, hate speech, deepfakes • Online radicalization by extremist groups • Mobilization of flash mobs, digital protests, communal violence • Espionage and use of fake profiles for identity theft or recruitment	• 2025: Fake Telegram channels sent bomb threats to 200+ Delhi schools • Deepfake videos circulated during 2024 elections • YouTuber arrested in 2025 for spying and leaking defence information

Government Measures to Tackle Challenges to Internal Security

Component	Key Government Measures	Examples / Initiatives
1. Communication Networks(cyber infrastructure, internet, telecom)	• Establishment of CERT-In (Indian Computer Emergency Response Team) for real-time cyber threat monitoring • National Cyber Coordination Centre (NCCC) for intelligence sharing • Cyber Swachhta Kendra for malware cleanup and digital hygiene • National Cyber Security Policy (revised draft 2023 under process) • Indian Telegraph Act amendments to intercept communication in public interest	• CERT-In's 2024 "Digital Threat Landscape Report" outlined surge in AI-based threats • NCCC helped neutralize cross-border cyberattacks on power sector in 2024 • National Cyber Exercise (NCX India) to train over 5,000 cybersecurity professionals
2. Traditional Media(TV, print, radio, digital news)	• Press Council of India to enforce media ethics and accountability • Electronic Media Monitoring Centre (EMMC) monitors TV content 24x7 Programme Code under Cable TV Networks Regulation Act, 1995 • PIB Fact Check Unit to counter fake news in mainstream media • Instructions to regulate airing of sensitive content during terror ops	• In 2024, I&B Ministry warned channels against airing communal content - Fake narratives during disasters (e.g. Manipur violence) were flagged by PIB Fact Check

3. Social Networking Sites(Twitter, WhatsApp, Telegram, etc.)	• **IT Rules, 2021** (amended in 2023) mandate platforms to appoint compliance officers, remove unlawful content within 72 hours • Blocking of harmful websites and social media handles under Section 69A of IT Act, 2000 • Indian Cyber Crime Coordination Centre (I4C) to track digital crimes across states • Use of AI tools like 'Garud Drishti' (Nagpur Police) to detect hate speech and fake news • Cyber crime helpline (1930) and portal (www.cybercrime.gov.in) for public grievance redressal	• In May 2025, 67 Pakistan-linked YouTube channels were blocked for spreading disinformation • Over 5 lakh fake social media accounts were taken down in 2024 (I4C data) • Cyber Support Centers set up in cities like Jaipur for psychological and legal aid to victims

Recent Development

Algorithmic Amplification of Extremism via Social Media

- **Introduction**
  - Social media algorithms have become central to content distribution and user engagement.
  - These algorithms, while aimed at enhancing user experience, often **inadvertently promote extremism**, disinformation, and polarisation—a phenomenon known as **algorithmic radicalisation**.
- **What is Algorithmic Radicalisation?**
  - The process by which **social media algorithms steer users into ideological extremes** by repeatedly promoting provocative or polarising content.
  - Users are led into "echo chambers" and "filter bubbles," reinforcing pre-existing beliefs and making them susceptible to extremist narratives.
- **How Algorithms Amplify Extremist Content**
  - **Engagement-Based Ranking**:
    - Content with high likes, shares, comments gets boosted.
    - Emotionally charged or controversial content is prioritised for higher engagement.
  - **Echo Chambers and Filter Bubbles**:
    - Repeated exposure to similar viewpoints prevents diverse perspectives, reinforcing radical views.
  - **Role of Hashtags**:
    - Hashtags enhance discoverability, helping extremist content reach targeted audiences.
  - **Targeted Personalisation**:
    - Machine learning models tailor feeds based on user behaviour, often pushing more extreme content to retain user attention.
- **Case Studies and Global Examples**
  - **Islamic State (IS) & Al-Qaeda**: Use platforms like X (Twitter), Telegram, and YouTube for recruitment and propaganda using coded language.
  - **Far-right Content on TikTok**: TikTok's "For You" feed promotes ideologically extreme content, especially to younger users.
  - **Election Disinformation**: Algorithms have been used to spread fake news and incite violence during democratic processes.
- **Challenges in Tackling Algorithmic Extremism**
  - **Algorithm Opacity**: "Black box" systems with little understanding even among developers.
  - **Evasive Tactics by Extremists**: Use of euphemisms, satire, and symbols to bypass detection.
  - **Cross-border and Cultural Gaps**: Global

algorithms often fail to account for **local socio-political contexts**.
    - **Balancing Free Speech and Regulation**: Risk of over-censorship vs. under-regulation (e.g., Germany's NetzDG law).
- **Mitigation Strategies**
    - **Technological Interventions**
        - **AI-Driven Moderation**:
            - YouTube's 2023 AI model reduced flagged extremist videos by 30%.
        - **Redirect Strategies**:
            - Platforms like Instagram redirect harmful searches to counter-narratives.
    - **Policy and Regulation**
        - **India's IT Rules, 2021**:
            - Mandate removal of flagged content within 36 hours.
            - Allow tracing of content originators.
        - **EU Digital Services Act, 2023**:
            - Mandates algorithm transparency and independent impact assessments.
        - **Germany's NetzDG Law**:
            - Requires platforms to remove hate speech within 24 hours, with heavy penalties.
- **Way Forward**
    - **Strengthen Public-Private Partnerships**: Joint efforts between governments, tech companies, and civil society are essential.
    - **Promote Algorithmic Transparency and Accountability**: Enact global standards for disclosure and compliance.
    - **Empower Users through Media Literacy**: Educate users to critically evaluate online content.

(The above topic is more related to the cybersecurity so we are going study more details in next topic.)

2 Basics of Cyber Security

Introduction

India's digital transformation—driven by over 795 million internet users, a thriving startup ecosystem, and emerging technologies like AI, cloud, and 5G—has enhanced connectivity and ambition. However, this growth has also expanded the cyber-attack surface, making cybersecurity and data privacy critical. Rising threats like ransomware, social engineering, and supply chain attacks underscore the need for integrated security and a **culture of cyber awareness** across all levels.

What is cybersecurity ?

Cybersecurity refers to the **practice of protecting internet-connected systems—including hardware, software, and data—from cyber threats**. It encompasses a set of technologies, processes, and practices designed to **safeguard networks, computers, mobile devices, and electronic data** from unauthorized access, attacks, damage, or theft.

- **Standard Definitions:**
  - **National Cyber Security Policy, 2013 (India):** "Cybersecurity is the protection of information, equipment, devices, computer systems and networks from unauthorised access, attacks, damage, disruption or destruction."
  - **NIST (U.S. National Institute of Standards and Technology):** "Cybersecurity is the process of protecting information by preventing, detecting, and responding to attacks."
  - **ITU (International Telecommunication Union):** "Cybersecurity refers to the collection of tools, policies, security concepts, risk management approaches, actions, training, best practices, assurance and technologies used to protect cyber environment.

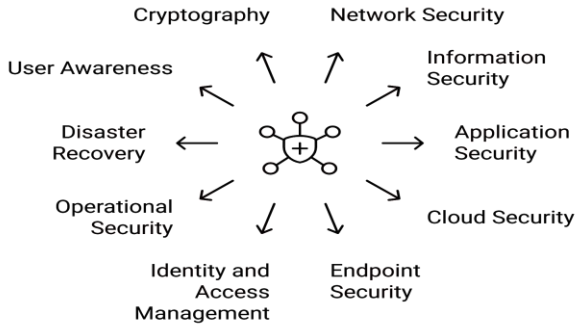
Elements of cybersecurity

Cybersecurity is a multi-dimensional framework comprising various interdependent components aimed at securing digital assets, networks, and infrastructure. The key elements include:

- **Network Security**
  - Protection of internal networks from unauthorized access, misuse, or disruptions using firewalls, intrusion detection systems, and virtual private networks (VPNs).
  - **Example:** Firewall blocking unauthorized access attempts on a government database.
- **Information Security (InfoSec)**
  - Ensures the confidentiality, integrity, and availability (CIA triad) of data—whether in storage, processing, or transit.
  - **Example:** Encrypting sensitive Aadhaar data to prevent leaks.
- **Application Security**
  - Involves identifying and fixing vulnerabilities in software and apps to prevent cyber attacks.
  - **Example:** Regular patching of government mobile apps like UMANG.
- **Cloud Security**
  - Protects data, applications, and infrastructure in cloud computing environments through encryption, identity management, and compliance tools.
  - **Example:** Securing sensitive health data hosted on cloud-based platforms like Ayushman Bharat Digital Mission.
- **Endpoint Security**
  - Secures individual devices like laptops, mobiles, and desktops from threats and exploits.
  - **Example:** Antivirus and device encryption on Election Commission EVMs and VVPATs.
- **Identity and Access Management (IAM)**
  - Ensures that only authorized individuals can access specific resources by using authentication tools like biometrics or OTPs.
  - **Example:** Aadhaar-enabled biometric verification in financial transactions.
- **Operational Security (OPSEC)**
  - Safeguards operational protocols and processes by identifying potential threats from routine actions.
  - Example: Rotating passwords and restricting data access based on roles in sensitive ministries.
- **Disaster Recovery and Business Continuity**
  - Strategies to restore operations and data access after cyber incidents or disruptions.

- **Example:** NIC's data recovery protocols post a ransomware attack.
- **User Awareness and Education**
  - Training individuals to recognize phishing, ransomware, and other threats to reduce human error.
  - **Example:** Cyber Surakshit Bharat Initiative for capacity building of officials.
- **Cryptography**
  - Use of encryption algorithms to secure communication and protect sensitive data.
  - **Example:** End-to-end encryption in government communication apps.

Cybersecurity Elements



Various Types of Cyber Attacks

- **Malware (Malicious Software)**
  - Software designed to harm or exploit systems, including viruses, worms, trojans, spyware, and ransomware.
  - Example: WannaCry ransomware attack (2017) affected Indian banking and healthcare systems.
- **Phishing Attacks**
  - Fraudulent emails or messages that trick users into revealing sensitive information like passwords or OTPs.
  - Example: Phishing emails pretending to be from the Income Tax Department during tax season.
- **Denial of Service (DoS) & Distributed Denial of Service (DDoS)**
  - Overloading a server or network with traffic to make it unavailable to legitimate users.
  - Example: DDoS attack on MEITY servers in 2022 causing temporary service disruption.
- **Man-in-the-Middle (MitM) Attack**
  - Attackers intercept and alter communication between two parties without their knowledge.
  - **Example:** Cybercriminals intercepting login credentials during online banking transactions.
- **SQL Injection**
  - Inserting malicious SQL code into input fields to access or manipulate backend databases.
  - **Example:** Breach of Indian university databases via SQL injection.
- **Zero-Day Exploit**
  - Exploiting unknown vulnerabilities in software before the developer releases a fix.
  - **Example:** Pegasus spyware used zero-day vulnerabilities in iOS/Android.
- **Credential Stuffing**
  - Automated use of leaked usernames and passwords to gain unauthorized access to user accounts.
  - **Example:** Attacks on Indian fintech and e-commerce sites using reused passwords.
- **Ransomware Attack**
  - Encrypts files and demands ransom for access restoration.
  - **Example:** AIIMS Delhi cyberattack (2022), where patient data was encrypted by hackers.
- **Cross-Site Scripting (XSS)**
  - Injecting malicious scripts into trusted websites, which then execute in users' browsers.
  - **Example:** Hackers targeting e-governance portals to steal session cookies.
- **DNS Spoofing**
  - Redirects traffic from legitimate websites to fake ones to steal credentials or install malware.
  - **Example:** Users redirected to fake banking websites during cyber frauds.
- **Social Engineering Attacks**
  - Manipulating people into giving up confidential information or performing actions that compromise security.
  - **Example:** Fraudsters posing as RBI officials to gain access to mobile OTPs.

Need of cybersecurity in india

- **Cybersecurity as a Core Internal Security Imperative**
  - India's internal security is increasingly challenged by **cyber intrusions**, which target **defense networks, financial institutions, communication infrastructure, and law enforcement databases**. From ransomware attacks paralyzing hospitals to data breaches affecting electoral rolls, these incidents can cause **mass disruption**, **social unrest**, and **loss of trust in governance**.
- **Surge in Cyberattack Volume and Complexity**
  - According to a **2024 PRAHAR study**, cyberattacks on India are projected to reach **1 trillion per annum by 2033**, potentially rising to **17 trillion by 2047**. This scale presents not only economic risk but also threats to **internal peace, stability, and national security**—particularly in sectors like power grids, air traffic control, and internal security databases.
- **Financial Sector Vulnerabilities**
  - The **Economic Survey 2024–25** reports that the **banking sector accounts for nearly one-fifth of all cyber incidents**, making it the most targeted sector. This threatens **economic security**, erodes public confidence in digital financial systems like UPI, and raises concerns about potential **cyber-induced financial crises**.
- **Institutional Unpreparedness**
  - As per **Cisco's 2023 Cybersecurity Readiness Index**, only **4% of Indian organizations are 'mature' in cyber resilience**. This lack of preparedness, particularly among critical public and private institutions, creates systemic vulnerabilities that can be exploited for **espionage, sabotage**, or **propaganda dissemination**, directly affecting law and order.
- **Enterprise-Level Threats and Operational Risks**
  - According to **CRN India**:
    - **80% of enterprises** in India have faced **ransomware attacks**.
    - **40% of large businesses** have experienced **phishing-led breaches**.
    - **92% fear operational disruption** due to ransomware—highlighting how **internal economic continuity and service delivery** are at risk.
- **Threats to Strategic and Military Infrastructure**
  - India's defense systems, intelligence platforms, and border surveillance increasingly rely on digital networks. These are lucrative targets for **state-sponsored cyber warfare**, **surveillance**, or **supply chain disruption**, with long-term implications for national security and internal law enforcement capabilities.
- **Citizen-Centric Security**
  - Digital governance systems like **Aadhaar, DigiLocker, and electoral databases** handle sensitive personal data. Breaches can lead to **identity theft**, **targeted misinformation**, and **social manipulation**—emerging forms of **non-conventional internal threats** undermining democratic institutions and civil liberties.

How Cyberspace Poses a Threat to National Security

- **Threats to Critical Infrastructure**
  - **Electric grids, nuclear plants, airports, and telecom networks** can be disrupted via cyberattacks, leading to blackouts, communication failure, or even accidents.
  - **Example:** In 2020, a suspected **Chinese-origin malware** attack reportedly targeted the **Mumbai power grid**, causing a major blackout.
- **Espionage and Intelligence Breaches**
  - State-sponsored actors exploit vulnerabilities to **steal sensitive defense, diplomatic, or economic data**.
  - **Example:** The 2022 breach of **All India Institute of Medical Sciences (AIIMS)** paralyzed hospital operations and raised concerns about medical data being weaponized.
- **Financial and Economic Disruption**
  - Cyberattacks on banks, stock exchanges, or digital payment platforms like UPI threaten **economic stability** and **public confidence**.

- As per **Economic Survey 2024–25**, almost **20% of reported cyber incidents** involved financial institutions.

- **Propaganda and Psychological Warfare**
  - Cyberspace is exploited to spread **fake news, deepfakes, hate speech**, and **polarizing content**, disturbing social harmony and public order.
  - **Example:** Use of **bot accounts and coordinated disinformation campaigns** during elections to influence voter behaviour and destabilize democratic processes.
- **Terrorism and Organized Crime Nexus**
  - Terrorist groups and drug cartels use encrypted platforms for **radicalization, fundraising (via crypto), logistics**, and **coordination of attacks**.
  - **Example**: The **2024 NIA anti-terror conference** flagged the growing use of **encrypted apps and darknet** for terror financing in Northeast India.
- **Border and Military Vulnerabilities**
  - Hackers can disable **satellite communication, drone systems, or border surveillance networks**, undermining India's defense preparedness.
  - **Example:** Pakistan-based groups have been linked to **cyber probes targeting Indian armed forces' networks**.
- **Cyber-enabled Insurgency and Left-Wing Extremism**
  - Insurgents increasingly use digital platforms to **recruit cadres, coordinate attacks**, and disseminate propaganda—especially in **LWE-affected and Northeastern regions**.
  - **Example:** The **"Urban Naxal" strategy** as per CPI (Maoist) documents, focuses on cyber outreach in cities.
- **Threats to Digital Sovereignty and Data Privacy**
  - Foreign tech platforms collect massive amounts of data from Indian users, raising concerns about **data colonization**, surveillance, and coercion.
  - **Example:** Bans on Chinese apps like **TikTok and WeChat** in 2020 were driven by national security concerns under **Section 69A of the IT Act**.

Challenges to Cybersecurity in India

- **Structural Challenges**
  - **Fragmented Cybersecurity Architecture:** India lacks a unified national cybersecurity command. Agencies like CERT-In, NCIIPC, IB, and NTRO often operate in silos, leading to poor coordination and duplication of efforts.
  - **Outdated Infrastructure:** Critical sectors like power, healthcare, and transport still operate on legacy systems that are highly vulnerable to cyber intrusions.
  - **Low Cyber Resilience in Private Sector:** According to Cisco's 2023 Cybersecurity Readiness Index, only **4% of Indian organisations** are at a 'mature' level of preparedness, highlighting systemic vulnerabilities in enterprise-level infrastructure.
- **Administrative Challenges**
  - **Jurisdictional Overlaps:** Cybercrime falls under both central and state jurisdictions, often causing confusion and delayed action due to lack of clarity in roles and responsibilities.
  - **Limited State Capacity:** Most state-level police forces lack dedicated cybercrime units or technical personnel to investigate sophisticated cyber offenses.
  - **Inadequate Enforcement of Existing Norms:** Despite frameworks like the National Cyber Security Policy (2013), implementation remains weak due to poor monitoring, limited funding, and bureaucratic inertia.
- **Human Resource-Related Challenges**
  - **Severe Talent Shortage:** As per a **World Economic Forum white paper**, India produces **one-third of the world's STEM graduates**, yet **30% of 40,000 cybersecurity jobs in 2024 remain unfilled** due to lack of industry-ready professionals.
  - **Skill Gaps and Poor Training Quality:** Existing technical education lacks hands-on training in areas like ethical hacking, cyber forensics, and threat intelligence. Public institutions are particularly under-equipped in this regard.
  - **Brain Drain and Urban Concentration:** Skilled professionals often migrate abroad or

join MNCs, leaving Indian government agencies under-resourced. Talent is also concentrated in metro cities, creating regional skill disparities.

- **Procedural Challenges**
  - **Delayed Incident Reporting:** Many organisations do not report breaches promptly due to reputational concerns, legal ambiguity, or lack of internal protocols, reducing response effectiveness.
  - **Weak Legal Enforcement:** Cybercrime laws under the IT Act, 2000 are outdated for dealing with modern threats like ransomware, crypto-crimes, and deepfakes. Prosecution is often slow and lacks technical support.
  - **Lack of Public Awareness:** Citizens and small businesses often fall prey to phishing, financial frauds, and identity theft due to poor cyber hygiene and limited awareness of digital safety norms.

Steps Taken by India Towards Cybersecurity

- **Legal and Policy Framework**
  - **Information Technology (IT) Act, 2000 (with 2008 amendments):** The primary law to combat cybercrime, hacking, identity theft, data breaches, and unauthorized access. It provides the legal basis for digital governance and penal provisions for cyber offenses.
  - **National Cyber Security Policy (NCSP), 2013:** Aimed at building secure and resilient cyberspace, this policy laid the foundation for capacity building, public–private partnerships, and institutional mechanisms. A **new National Cybersecurity Strategy** is under draft consideration (by NSCS) as of 2024.
  - **Digital Personal Data Protection Act, 2023:** A landmark legislation that establishes **data fiduciary responsibilities**, consent architecture, and grievance redressal mechanisms to ensure privacy and security of citizen data.
  - **Indian Telecommunication Act, 2023 (draft):** Proposes stricter norms for securing telecom infrastructure and combating cyber threats via internet-based communication services.
  - **CERT-In Guidelines (2022):** Mandate reporting of cyber incidents within 6 hours, require log retention, and enforce stricter VPN/data center compliance to improve incident response.
- **Institutions and Agencies**
  - **CERT-In (Indian Computer Emergency Response Team):** The national nodal agency for responding to cybersecurity incidents, coordinating alerts, advisories, and vulnerability assessments.
  - **NCIIPC (National Critical Information Infrastructure Protection Centre):** Under the National Technical Research Organisation (NTRO), responsible for securing critical sectors such as power, banking, telecom, and transport.
  - **National Cyber Coordination Centre (NCCC):** Operated by the Ministry of Home Affairs to scan internet traffic in real-time and coordinate cyber threat intelligence.
  - **Indian Cyber Crime Coordination Centre (I4C):** Established in 2020 under MHA to coordinate cybercrime investigations, maintain a national cybercrime reporting portal, and support state cyber units.
  - **Data Protection Board (under DPDP Act 2023):** A statutory body for adjudicating data protection breaches and ensuring compliance with data privacy norms.
  - **Defence Cyber Agency (DCA):** Set up under the Ministry of Defence to address military-level cyber warfare, digital espionage, and offensive/defensive cyber operations.
- **Key Programs and Initiatives**
  - **Cyber Surakshit Bharat (launched in 2018):** A public–private campaign to promote awareness and build capacity among government officials, especially in critical ministries and state governments.
  - **National Cyber Crime Reporting Portal (cybercrime.gov.in):** A 24x7 portal for citizens to report cyber frauds, financial scams, and cyberbullying anonymously.
  - **Cyber Swachhta Kendra:** Botnet Cleaning and Malware Analysis Centre that provides free security tools to detect and remove malicious software.
  - **Digital Intelligence Platform (Proposed):** A new initiative to create a centralised data

analytics platform integrating inputs from law enforcement, CERT-In, and NCCC.

- **Secure India Campaign (Upcoming, 2025):** Proposed mass awareness drive focusing on citizen cyber hygiene, AI-related cyber threats, and misinformation countermeasures.
- **Partnerships with Industry and Academia:** Initiatives like the **Cyber Security Grand Challenge (MeitY)** and collaboration with **IITs/NITs** to develop indigenous cybersecurity tools and workforce.
- **International Engagements:** India is an active participant in **Global Forum on Cyber Expertise (GFCE)**, **No Money For Terror (NMFT)** summits, and bilateral cyber dialogues with countries like the US, Japan, and Australia.

International Best Practices for Cybersecurity

- **Comprehensive National Cybersecurity Strategies**
  - **United States – National Cyber Strategy (2023):** Emphasizes "defend forward" doctrine, integrating cyber offense as a deterrence tool. Includes public-private threat intelligence sharing and strict accountability for software providers.
  - **United Kingdom – National Cyber Strategy (2022):** Prioritizes public-private collaboration, education & training (Cyber First Programme), and international law-based cyber diplomacy. The UK also has a dedicated **National Cyber Security Centre (NCSC)** under GCHQ.
  - **Singapore – Cybersecurity Strategy 2021:** Focuses on operational technology (OT) security, critical infrastructure protection, and regional cyber capacity building via ASEAN frameworks.
  - **Israel – National Cyber Directorate:** Integrates military, civilian, and industrial sectors into a single cyber ecosystem. Known for developing world-class talent and startups in cybersecurity.
- **Strong Legal and Regulatory Architecture**
  - **EU General Data Protection Regulation (GDPR):** Sets a global standard for data privacy, ensuring informed consent, right to be forgotten, and heavy penalties for non-compliance.
  - **USA – Cyber Incident Reporting for Critical Infrastructure Act (2022):** Mandates cyber incident reporting within 72 hours and ransom payments within 24 hours for critical sectors.
  - **Japan – Act on the Protection of Personal Information (APPI):** Combines data localization with business flexibility and cross-border data transfer standards, balancing innovation with privacy.
- **Cybersecurity Workforce Development**
  - **Estonia – Cybersecurity Skills Framework:** Integrated with national education policy; Estonia promotes coding and cybersecurity from the school level.
  - **UK's CyberFirst & Cyber Discovery programs:** Nurture cybersecurity talent from school to university, linking students with government and private internships.
  - **Israel – Talpiot and Unit 8200 Model:** Elite military training unit that produces cyber experts who later transition into academia, government, or private startups.
- **Global Norms and Multilateral Engagements**
  - **Budapest Convention on Cybercrime (2001):** First international treaty seeking harmonization of laws and cooperation on cybercrime investigation. Over 65 countries are signatories (India is not yet a member).
  - **Paris Call for Trust and Security in Cyberspace:** Advocates responsible state behavior, non-targeting of critical infrastructure, and cyber capacity building in the Global South.
  - **United Nations OEWG and GGE Platforms:** Promote voluntary norms of responsible behavior in cyberspace, including non-use of cyber tools for political coercion or warfare.
- **Cyber Diplomacy and Deterrence**
  - **European Union – Cyber Diplomacy Toolbox:**

Allows diplomatic sanctions (e.g., travel bans, asset freezes) against foreign entities engaged in cyberattacks.
    - **NATO – Cyber Defence Pledge:** Recognizes cyber as a domain of warfare; enhances collective defense commitments in the face of cyber threats.
    - **United States – Attribution and Countermeasures Doctrine:** Publicly attributes cyberattacks to specific nations (e.g., China, Russia, Iran) and uses legal/financial sanctions to deter further aggression.
- **Key Takeaways for India**
    - **Adopt incident reporting mandates** and cyber-insurance standards similar to the USA and EU.
    - **Accelerate cyber workforce development** through national scholarships, internships, and coding education in schools.
    - **Institutionalize public-private cooperation** by creating sector-specific cyber cells linked to CERT-In and NCIIPC.
    - **Consider joining the Budapest Convention** to enhance international cooperation on cybercrime investigations.
- **Develop cyber deterrence capabilities** and a legal doctrine on state-sponsored cyber threats, similar to NATO and the US.

Recent Development

United Nations Convention on Cybercrime

Context

- In a landmark development, the **United Nations General Assembly** has adopted the **first-ever legally binding UN convention on cybercrime**, marking a significant step in global efforts to combat digital threats.

Key Facts

- **Adoption**: Unanimously adopted by all **193 UN Member States**.
- **Signing Venue**: The convention will be opened for signature in **Hanoi, Vietnam**, in 2025.
- **Secretariat**: The **United Nations Office on Drugs and Crime (UNODC)** will serve as the permanent secretariat.
- **Enforcement Trigger**: The convention will come into effect once **40 countries ratify or accede to it**.

Scope and Purpose

- Focuses on the **prevention, investigation, and prosecution** of cybercrimes.
- Provides a legal framework for the **freezing, confiscation, and return of crime proceeds** derived from cyber activities.
- Facilitates **collection, preservation, and sharing of electronic evidence** in criminal cases.

Key Provisions

- **International Cooperation and Data Sharing**
    - Establishes a 24/7 contact network for **immediate assistance** between states.
    - Encourages **mutual legal assistance** and **extradition agreements**.
    - Facilitates **cooperation for asset confiscation and recovery**.
- **Procedural Guidelines for Law Enforcement**
    - Provides standards for the **preservation, search, seizure, and collection of electronic evidence**.
    - Promotes the creation of specialized cybercrime investigation units.
- **Data Privacy and Protection**
    - Mandates that data sharing must comply with **national privacy laws**.
    - Encourages **bilateral/multilateral frameworks** to enable secure and lawful data transfer.
    - Includes **safeguards against misuse** of personal data during cross-border investigations.
- **Protection of Human Rights**
    - Affirms that implementation of the convention must be consistent with **international human rights obligations**, including rights to **privacy, fair trial, and freedom of expression**.
- **Additional Provisions**
    - Includes mechanisms for:
        - **Extradition of cybercriminals**
        - **Transfer of sentenced persons**

- **Transfer of criminal proceedings**
- **Conduct of joint investigations** across jurisdictions

Significance

- Fills a critical global gap in the fight against **transnational cybercrime**.
- Strengthens legal cooperation among nations, especially in areas like **ransomware attacks, online fraud, and digital espionage**.
- Balances **state sovereignty, security concerns, and human rights obligations**.

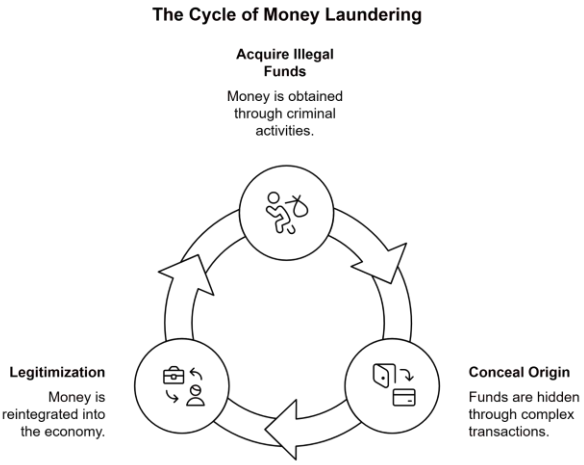
3 Money Laundering

Introduction

In today's globalized economy, money laundering is not only a major economic offence but also a **serious national security threat**, as it often finances terrorism, organized crime, drug trafficking, and tax evasion—undermining the integrity of financial systems and governance structures.

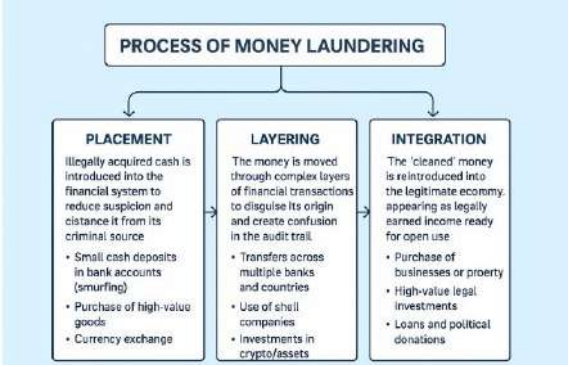
What is money laundering ?

- **Money laundering** is the process of concealing the origins of illegally obtained money by making it appear as though it has come from a legitimate source.



- As per **Section 3 of the Prevention of Money Laundering Act (PMLA), 2002**: *"Whosoever directly or indirectly attempts to indulge or knowingly assists or is a party or is actually involved in any process or activity connected with the proceeds of crime including its concealment, possession, acquisition or use and projecting or claiming it as untainted property shall be guilty of offence of money-laundering.*

Process of Money Laundering



Various Techniques and Methods Used in Money Laundering

Category	Technique	Explanation
1. Cash-Based Methods	**Smurfing (Structuring)**	This involves breaking large amounts of illicit cash into smaller deposits (usually below reporting limits) and depositing them into various bank accounts. The aim is to avoid triggering scrutiny by financial institutions or regulators.
	Bulk Cash Smuggling	Physically carrying large amounts of cash across borders—often hidden in bags, vehicles, or through couriers—to move it out of the country or into another financial system where checks are weaker.
	Cash-Intensive Businesses	Criminals invest in businesses like restaurants, bars, or casinos where cash transactions are common. They then mix illegal cash with daily business revenue to make it appear legitimate.
2. Use of Financial Systems	**Trade-Based Money Laundering (TBML)**	Criminals manipulate trade documents (like invoices) by over-invoicing or under-invoicing goods or services. For example, showing ₹10 crore worth of goods as ₹1 crore to shift money across borders.

	Shell Companies	These are fake or inactive companies that have no real business activity. They are used to move and hide illegal money while masking the identity of the true owner.
	Round-Tripping	Money is sent abroad (often to tax havens) through fake business deals and then brought back into the country as "foreign investment" or "business income" to make it appear clean.
	Wire Transfers and Multiple Account Transfers	Using rapid electronic fund transfers through several domestic and international bank accounts to make the origin and trail of the money confusing.
3. Asset Conversion	**Real Estate Transactions**	Criminals buy property using black money, and later sell it—declaring it as profit or capital gain. Sometimes, the purchase and sale prices are deliberately inflated or deflated to facilitate laundering.
	Luxury Goods and Art	Buying expensive items such as gold, paintings, watches, or cars to convert cash into physical assets. These can be stored, resold, or transported easily without much scrutiny.
	Cryptocurrencies	Digital currencies like Bitcoin offer anonymity and are used to move money across borders or hide illegal funds. Transactions are harder to trace and regulation is still evolving.
4. Informal and Illicit Channels	**Money Mules**	Individuals (knowingly or unknowingly) are recruited to transfer money through their bank accounts or in person. This makes tracking the actual criminal difficult. Often used in cybercrimes and scams.
	Hawala or Informal Value Transfer System	An unofficial method where money is transferred through a network of brokers without actual movement of cash. It operates on trust and leaves little documentary evidence.
	Gambling and Betting	Illicit money is used for betting or gambling, and the winnings are shown as legal income. Online betting platforms are increasingly used for this purpose.

Impact of Money Laundering on the Nation

- **Undermines Financial Integrity and Institutions**
  - Money laundering distorts the functioning of financial institutions by introducing illicit money into the system.
  - It weakens banks' risk assessment and transparency, making them vulnerable to blacklisting and sanctions.

- **Example:** Non-compliance with FATF standards can lead to greylisting, as happened with Pakistan.

- **Encourages Corruption and Criminal Economy**
  - It fuels the growth of parallel economies and black markets, reducing the effectiveness of monetary and fiscal policies.
  - Encourages corruption among officials and bureaucrats who help conceal such activities, eroding institutional trust.
- **Reduces Tax Revenue and Government Capacity**
  - Laundered money often escapes taxation, leading to significant losses in public revenue.
  - This limits the government's ability to invest in welfare programs, infrastructure, and public services.
- **Destabilizes Real Estate and Commodity Markets**
  - Real estate is a common channel for laundering money, resulting in **artificial inflation of property prices**, making housing unaffordable for the middle class.
- **Facilitates Terror Financing and Organized Crime**
  - Laundered funds are often used to finance terrorism, insurgency, arms smuggling, and drug trafficking.
  - Example: The 2024 NIA conference highlighted links between organized crime, terror financing, and illicit financial flows in Northeast India.
- **Distorts Investment and Market Competition**
  - Legitimate businesses lose out to front companies and shell firms supported by laundered capital, leading to **unfair competition** and economic inefficiency.
- **Threatens International Reputation and Investor Confidence**
  - Countries perceived as safe havens for money laundering face **capital flight, poor credit ratings**, and loss of foreign investment.
  - **Example:** Nations with weak anti-money laundering controls often attract scrutiny from FATF and the global banking system.
- **Erodes Rule of Law and Governance**
  - When crime proceeds are legitimized, it undermines the authority of legal systems and encourages **criminal infiltration into politics and bureaucracy**.

Legal and Institutional Framework to Tackle Money Laundering in India

1. Legal Framework

- **Prevention of Money Laundering Act (PMLA), 2002**
  - **Primary legislation** to combat money laundering and confiscate proceeds of crime.
  - Defines offences and lays down procedures for attachment, adjudication, and confiscation of property.
  - Empowers ED to conduct investigations, arrest accused, and provisionally attach properties.
- **Benami Transactions (Prohibition) Act, 1988 (amended in 2016)**
  - Prohibits benami (proxy) ownership of properties.
  - Empowers authorities to confiscate benami properties used to park black money or launder funds.
- **Foreign Exchange Management Act (FEMA), 1999**
  - Regulates foreign exchange transactions.
  - Helps monitor and prevent cross-border movement of illegal funds.
- **Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015**
  - Targets concealment of foreign assets and incomes by Indian residents.
  - Includes strict penalties and prosecution provisions.
- **Companies Act, 2013**
  - Mandates disclosures of **Beneficial Ownership** and prohibits **shell companies**.
  - Enhances compliance and transparency in corporate financial practices.
- **Narcotic Drugs and Psychotropic Substances Act (NDPS), 1985**
  - Recognizes laundering of drug proceeds as a criminal offence.

2. Institutional Framework

- **Enforcement Directorate (ED)**
  - Nodal agency under the Department of Revenue for investigating offences under PMLA.

- Empowered to attach assets, arrest offenders, and file complaints before special courts.
- **Financial Intelligence Unit - India (FIU-IND)**
  - Under the Finance Ministry, it receives, analyzes, and disseminates suspicious financial transaction reports (STRs) from reporting entities (banks, NBFCs, etc.).
  - Plays a central role in tracking laundering patterns and inter-agency coordination.
- **Reserve Bank of India (RBI)**
  - Enforces **Know Your Customer (KYC)**, **Anti-Money Laundering (AML)**, and **Combating Financing of Terrorism (CFT)** guidelines for banks and financial institutions.
- **Securities and Exchange Board of India (SEBI)**
  - Monitors money laundering risks in the capital markets.
  - Issues AML compliance guidelines to intermediaries like brokers and mutual funds.
- **Central Board of Direct Taxes (CBDT) and Central Board of Indirect Taxes and Customs (CBIC)**
  - Investigate tax evasion, hawala transactions, and illicit cross-border fund flows.
- **National Investigation Agency (NIA)**
  - Investigates terror funding cases involving laundering of funds through organized crime or foreign handlers.
- **Central Economic Intelligence Bureau (CEIB)**
  - Coordinates intelligence among various economic enforcement agencies to counter money laundering and financial crimes.

3. International Cooperation

- India is a member of the **Financial Action Task Force (FATF)** and its regional body **Asia/Pacific Group (APG)**.
- Bilateral treaties for information exchange, **Mutual Legal Assistance Treaties (MLATs)**, and **Tax Information Exchange Agreements (TIEAs)** help track and recover illicit assets abroad.

Black Money

What is black money ?

- There is no official definition of black money in economic theory, with several different terms such as parallel economy, black money, black incomes, unaccounted economy, illegal economy and irregular economy all being used more or less synonymously. The simplest definition of black money could possibly be money that is hidden from tax authorities.

Factors contribute to the generation of black money:

- **Tax Evasion:** Underreporting income, inflating expenses, and fraudulent practices to evade taxes generate black money.
- **Corruption:** Bribes and kickbacks received or given in exchange for favors contribute to black money generation.
- **Unregulated Cash Transactions:** Undeclared cash payments for goods, services, or property transactions generate black money.
- **Illegal Activities:** Illicit activities like drug trafficking, smuggling, and arms trade generate illegal income and black money.
- **Offshore Accounts and Money Laundering:** Black money is concealed through offshore accounts and money laundering techniques.
- **Parallel Economy:** Unregistered businesses, unreported income, and transactions outside official records contribute to black money generation.

Challenges in Curbing Black Money

- **Lack of Transparency:** Black money transactions occur outside the formal financial system, making it hard to trace and identify those involved.
- **Cross-Border Transactions:** Black money moves across borders, exploiting differences in regulations and jurisdictions, requiring international cooperation.
- **Complex Money Laundering Techniques:** Sophisticated methods like layering transactions and using offshore accounts make it challenging to detect and prove the origins of black money.
- **Informal Economy:** Black money thrives in the informal sector, which operates outside official records and regulations.
- **Corruption and Bribery:** Black money is intertwined with corruption, necessitating efforts to tackle corruption and enforce anti-bribery

measures.
- Technological Advancements: Advancements like cryptocurrencies and encrypted communication channels provide new avenues for black money transactions that are difficult to track.

Way forward
- Strengthen legal frameworks and penalties.
- Foster international cooperation and information exchange.
- Enhance financial transparency through monitoring and technology.
- Strengthen enforcement capabilities against black money.
- Promote tax compliance through simplification and awareness.
- Facilitate financial inclusion to reduce the informal sector.
- Encourage public participation and protect whistleblowers.
- Promote transparency, accountability, and ethics

Recent Development

<u>FATF Mutual Evaluation Report on India (2024)</u>

Context
- In June 2024, the **Financial Action Task Force (FATF)**, the global watchdog for money laundering and terror financing, released its **Mutual Evaluation Report (MER)** on India during its plenary session held in **Singapore**.
- India was placed in the **"regular follow-up" category**, the highest rating assigned by FATF. Among federal economies, India is the only major country to have achieved this rating, joining a select group including the UK**, France, and Italy**.

FATF Follow-Up Categories (Post-Mutual Evaluation)

Category	Description	Implication
Regular Follow-Up	High compliance, minimal deficiencies	Periodic updates; highest rating
Enhanced Follow-Up	Moderate deficiencies	Frequent reporting; closer monitoring
Grey List	Strategic AML/CFT weaknesses	Increased global scrutiny
Black List	Severe non-compliance	Global counter-measures and isolation

Key Highlights of the FATF Report

1. Areas of Strength and Acknowledgment
- **High Technical Compliance**: India met most FATF standards with strong legal and institutional frameworks to tackle money laundering and terror financing.
- **Effective Institutional Action**:
  - Recognized the **Enforcement Directorate (ED)** and **National Investigation Agency (NIA)** for concrete actions against terror financing.
- **Financial Inclusion Measures**:
  - Acknowledged the success of the **Jan Dhan-Aadhaar-Mobile (JAM) Trinity**, and rapid expansion of **digital payments** in enhancing financial transparency.
- **Tax and Billing Reforms**:
  - Praised the implementation of **GST**, **e-invoicing**, and **e-billing**, contributing to supply chain traceability and curbing financial fraud.

2. Areas Requiring Improvement
- **Non-Profit Organisations (NPOs)**:
  - Charitable institutions receiving tax exemptions are seen as **vulnerable to terror financing**. Stronger risk assessments and monitoring are recommended.
- **Politically Exposed Persons (PEPs)**:
  - There is **ambiguity** in defining domestic PEPs and identifying the **source of funds, wealth, and beneficial ownership**. A clearer legal definition and enhanced scrutiny are needed.
- **Designated Non-Financial Businesses and Professions (DNFBPs)**:
  - Regulatory and supervisory **gaps** exist, particularly in the **real estate and precious metals & stones (PMS)** sectors.
  - Despite PMS accounting for **7% of GDP**, only **9,500 of 1.75 lakh** dealers are registered with the **Gems and Jewellery Export Promotion**

Council (GJEPC).

3. Sector-Specific Vulnerabilities

- **Money Laundering Risks**:
  - Domestic crimes such as **fraud, cybercrime, drug trafficking, and corruption** remain primary sources of laundered funds.
  - **Precious metals and stones (gold, diamonds)** are particularly misused due to weak ownership trails and high value.
- **Terrorist Financing Threats**:
  - Threats stem from **Islamic State (ISIL), Al-Qaeda affiliates in Jammu & Kashmir**, and **Left-Wing Extremist** and **Northeast insurgent groups**.
  - While preventive steps are in place, **prosecution and conviction** rates for terror financing remain low.

FATF Recommendations to India

- **Expedite Pending Trials**: Fast-track money laundering and terror financing cases, particularly those involving **drug crimes and human trafficking**.
- **Enhance Sanction Framework**: Implement **targeted financial sanctions** more efficiently, including rapid freezing of funds and effective inter-agency communication.
- **Define and Regulate Domestic PEPs**: Legally recognize domestic politically exposed persons and enforce **risk-based enhanced due diligence**.
- **Improve Risk Mapping in PMS Sector**: Deepen qualitative and quantitative data gathering on risks related to **gold and diamond smuggling**.

Implications for India

Area	Impact
International Cooperation	Improved FATF status boosts India's ability to cooperate on **cross-border financial crimes**, aiding in **asset recovery** (e.g., cases like Vijay Mallya, Nirav Modi).
Global Financial Access	Better FATF compliance improves India's credibility in **global borrowing and financial markets**, facilitating access to international capital.
Digital Diplomacy	Enhances India's case for global expansion of **UPI** as a reliable cross-border digital payments solution.
Investor Confidence	Strengthens foreign investor trust in India's regulatory environment, contributing to **FDI inflows and financial market stability**.

Value Addition

Keyword : Communication Networks, Social Networking Sites, Internal Security, Cyberattacks, Disinformation, Cybercrime, Algorithmic Radicalization, Echo Chambers, Deepfakes, Hate Speech, Cyber Hygiene, Cybersecurity, Critical Infrastructure, Terror Financing, Money Laundering, Shell Companies, Black Money, FATF, Data Privacy, Digital Sovereignty, Internet of Everything

Mains Practice Questions :

Q1. Analyze the impact of deepfakes and misinformation on democratic institutions. How effective are India's regulatory frameworks in curbing these threats?

Q2. What is algorithmic radicalization? How do social media algorithms amplify extremist content and threaten internal stability?
India's growing digital footprint has increased its vulnerability to cyber threats. Discuss with reference to recent incidents.

Q3. Critically assess the role of international cooperation and treaties in India's cybersecurity strategy. Should India consider joining the Budapest Convention?

Q4. Explain the process of money laundering and its impact on internal security. How effective is the PMLA in curbing it?

Q5. Discuss the interlinkage between money laundering, terror financing, and organized crime. Illustrate with Indian examples.

In news

- **Sharing sensitive information with Foreign adversary**
  - Recently, Maharashtra ATS arrested a Thane resident and two associates for sharing sensitive information with Pakistani Intelligence Operatives via social media, highlighting espionage risks.
- **Propaganda on Telegram**
  - Recently, NIA intercepted propaganda on Telegram by terror groups like AQIS and LeT, targeting youth for radicalization and recruitment, underscoring social media's role in cyberterrorism
- **Risks related to cybersecurity, AI and other emerging technologies**
  - according to the latest Institute of Internal Auditors (IIA) – Protiviti India Survey 2025, New governance risks related to cybersecurity, Artificial Intelligence (AI) and other emerging technologies have emerged as most critical in risk management for enterprises, by a majority of internal audit professionals
- **Cyber Commandos**
  - Union Home Minister announced , Centre aims to train and prepare 5,000 'Cyber Commandos' over the next five years in a bid to tackle the growing concerns around the rise of cybercrime.
- **Money Laundering through online Gaming**
  - Recently, a Digital India Foundation report identified money laundering as a major threat to India's online gaming sector, recommending a government whitelist of compliant gaming companies to ensure payment gateways and ISPs serve only authorized operators.

Acronym

CYBERNET

(Covers cyber and communication network-related threats)

- **C – Cyber Attacks** (Malware, ransomware, critical infrastructure hacks)
- **Y – Yielding Fake News** (Through social media manipulation)
- **B – Botnets & Deepfakes** (Mass misinformation, impersonation threats)
- **E – Encryption Misuse** (End-to-end tools used by terror/crime)
- **R – Radicalization Online** (Extremist content dissemination)
- **N – Network Vulnerabilities** (Undersecured digital infrastructure)
- **E – Espionage & Surveillance** (Data leaks, spying)
- **T – Terror Coordination via Encrypted Apps**

VIRAL

(Focus on role of media and social networking sites in internal security)

- **V – Viral Misinformation** (Spreads panic, communal hatred)
- **I – Incitement of Violence** (Hate speech, mob mobilization)
- **R – Rumor Propagation** (Undermines state authority)
- **A – Anonymity Exploited** (Trolls, cyberbullying, extremist handles)
- **L – Lack of Regulation** (Grey areas in digital governance)

LAUNDER

(For Money Laundering and Prevention)

- **L – Layering of Transactions** (Key step in laundering)
- **A – Anonymous Shell Companies**
- **U – Underground Banking (Hawala)**
- **N – Nexus with Crime/Terror**
- **D – Detection Mechanisms (FIU-IND, STRs)**
- **E – Enforcement Agencies (ED, FATF Compliance)**
- **R – Regulatory Framework (PMLA, AML norms)**

Ready-made template for Intro-Conclusion

<u>Challenges to Internal Security through Communication Networks, Role of Media and Social Networking Sites in Internal Security Challenges, Basics of Cyber Security</u>

INTRODUCTIONS:

- **Integrated Intro (All topics):**
  In a 'New India', where digital infrastructure is the backbone of governance, economy, and society, internal security threats have migrated to the virtual world. Cybercrime, digital misinformation, money laundering via encrypted channels, and unregulated media now challenge state stability like never before.

- **Cyber Battlefield Framing:**
  Cyberspace is the new battlefield."
  India's internal security today hinges on mastering this domain — from tackling digital radicalization to preventing online money laundering, the war is wired.

- **Tech Angle with Call to Action:**
  As India aspires to become a $5 trillion digital economy, the lack of cyber awareness, inadequate surveillance over social media, and weak financial digital trails pose major risks. Cyber-responsible citizens, businesses, and governments are the need of the hour.

- **Media-Centric Intro:**
  Social media, once a tool of empowerment, is now a double-edged sword. Misinformation, deepfakes, and propaganda campaigns are destabilizing peace and security. A 'Super Cyber Force' is needed to protect India's digital democracy.

CONCLUSIONS:

- **Strategic Outlook:**
  Cyber threats respect no borders. To defend New India, we must go beyond passive defense—cyber surveillance, offensive capabilities, AI-driven monitoring, and digital education must be national priorities.

- **Call for Resilience:**
  Digital freedom must not come at the cost of national security. Whitelisting platforms, educating netizens, and cracking down on digital money laundering are essential to preserve internal peace.

- **Quote-Based:**
  "In the age of information, ignorance is a security threat."
  From fake news to financial fraud, India must secure its digital frontier with skill, strength, and strategy.

- **Policy Focused:**
  The integration of cyber cells, financial monitoring agencies, and tech companies is vital. Multi-stakeholder collaboration is the only sustainable firewall for internal security.

<u>Money-Laundering and its prevention.</u>

Improved Introduction :

- **Quote + Data-Based:**
  "Follow the money" has never been more urgent. According to ED data, over **₹1 lakh crore** is under investigation under PMLA. Money laundering today is not just financial fraud—it's the invisible engine behind terror, drugs, and organized crime in India.

- **Digital + Data Framing:**
  With the ED filing over **5,000 PMLA cases** and low conviction rates (~0.75%), India's money laundering problem is both massive and persistent. The rise of cryptocurrency, shell firms, and darknet transactions adds new layers to this internal security threat.

- **Security + Financial Fusion:**
  India's internal security is increasingly compromised by financial crimes. High-profile cases like the **Mahadev Betting App scam (₹40,000 crore)** reveal how laundering networks fund cross-border terror, election manipulation, and social unrest.

- **Contemporary Context with Numbers:**
  In the last decade, money laundering has evolved into a tech-savvy, borderless threat. With thousands of crores funneled through fake accounts and crypto wallets, India faces not just economic loss but a serious national security risk.

Revised Conclusions :

- **Strategic + Specific:**
  India must enhance the effectiveness of PMLA enforcement, improve inter-agency data sharing, and use blockchain for real-time tracking. Stronger international treaties are needed to repatriate laundered money and break global terror-finance chains.

- **Quote + Policy Call:**
  "Dirty money fuels dirty deeds."
  To cut off the financial lifeline of anti-national elements, India must blend financial intelligence with national security operations—especially in high-risk sectors like betting, real estate, and digital payments.

- **Digital Security Lens:**
  ech-driven money laundering requires tech-driven solutions. AI surveillance, digital KYC norms, and cross-border fintech scrutiny are essential to prevent the misuse of India's growing digital economy.

- **Action-Oriented:**
- From Dubai-based fraud networks to crypto-driven scams, the money trail is global and fast. India must act with speed—through legal, diplomatic, and technological means—to secure its economy and sovereignty.

Control of social networking sites and media threats.

Heading	Subheadings
Social control	• Civil society activism • Social harmony measures • Influencers
Economic control	• Responsible intermediaries • Monetising threats • Inclusive development
Political control	• Legislation • Counter propoganda • E-governance • Social media campaigns
Technological control	• Modern technology • Reasearch and development • Fact checkers

5 UNIT Security Challenges and their Management in Border Areas

Navigating the Syllabus: What You Need to Know

Security Challenges and their Management in Border Areas

- Challenges along various borders of India
  - Land Border
  - Coastal Border
- Land Boundary disputes with Neighbours India's Border Policy
- Solution

UPSC Previous year Questions

Question	Nature of Question	Core Demand
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. (2024)	China-Pakistan Borders + Infrastructure Schemes	Examine disputes and security challenges; outline BADP & BIM schemes
For effective border area management, discuss the steps required to be taken to deny local support to militants and also suggest ways to manage favourable perception among locals. (2020)	Perception Management + Counter-Insurgency	Suggest steps to prevent local militant support and build positive perceptions
Analyze internal security threats and trans border crimes along Myanmar, Bangladesh and Pakistan borders including Line of Control (LoC). Also discuss the role played by various security forces in this regard. (2020)	Border Threats + Security Forces Role	Discuss threats along 3 borders and role of security forces
Cross-Border movement of insurgents is only one of the several security challenges facing the policing of the border in North-East India. Examine the various challenges currently emanating across the India-Myanmar border. Also, discuss the steps to counter the challenges. (2019)	India-Myanmar Border Challenges	Explain insurgent challenges and countermeasures at India-Myanmar border

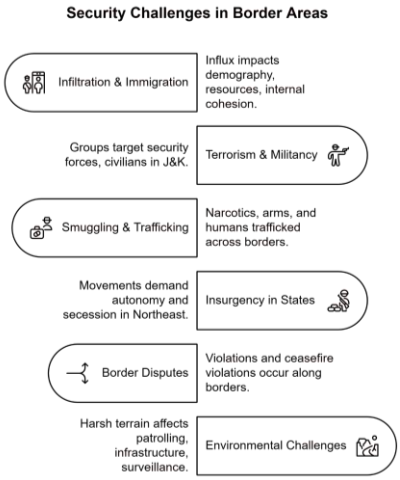
The terms 'Hot Pursuit' and 'Surgical Strikes' are often used in connection with armed action against terrorist attacks. Discuss the strategic impact of such actions. (2016)	Strategic Military Response	Evaluate impact of surgical strikes and hot pursuit on national security
Border management is a complex task due to difficult terrain and hostile relations with some countries. Elucidate the challenges and strategies for effective border management. (2016)	Border Challenges + Management Strategies	List terrain and diplomatic challenges and effective border strategies
How does illegal trans border migration pose a threat to India's security? Discuss the strategies to curb this, bringing out the factors which give impetus to such migration. (2014)	Illegal Migration + National Security	Explain threat from illegal migration and steps to curb it
China and Pakistan have entered into an agreement for development of an economic corridor. What threat does this pose for India's security? Critically examine. (2014)	CPEC + Strategic Concerns	Critically assess CPEC's strategic threat to India
How far are India's internal security challenges linked with border management particularly in view of the long porous borders with most countries of South Asia and Myanmar? (2013)	Border Management + Internal Security Link	Explain how porous borders intensify internal security threats

1 Land Border Management

Introduction

- **According to the United Nations Security Council**, border management is indeed considered the first line of defense against several threats, including the movement of terrorists across borders and the illegal cross-border movement of goods and cargo
- Securing India's land borders is a strategic imperative central to its national security, sovereignty, and regional stability. With over 15,000 kilometers of international borders spanning some of the world's most volatile frontiers—from the Line of Control with Pakistan to the contested Line of Actual Control with China—India faces persistent and evolving threats.
- The sheer diversity of terrain and the geopolitical sensitivities surrounding these borders make their management both complex and critical.
- Effective land border management is thus essential not only to counter external threats but also to promote internal cohesion and balanced development in border areas.

Nature of Security Challenges in Border Areas



Challenges in Effective Border Management in India

- **Geographical and Terrain-Related Challenges**
  - **Difficult topography** such as high-altitude Himalayan terrain (e.g., Ladakh, Arunachal Pradesh), dense forests (e.g., Assam, Nagaland), and marshy lands (e.g., Rann of Kutch) hinders physical surveillance.
  - **Riverine and porous borders** in regions like West Bengal and Assam complicate fencing and patrolling.
  - **Adverse weather conditions** (snowfall in J&K, floods in Assam) restrict access and deployment.
- **Porous and Unfenced Borders**
  - **Bangladesh and Myanmar borders** have several stretches that remain unfenced or broken due to land disputes, local resistance, or difficult terrain.
  - **Nepal and Bhutan borders** follow an open-border policy, making regulation of movement more complex.
  - **Example:** The Indo-Bangladesh border sees frequent cross-border smuggling and illegal migration.
- **Cross-Border Infiltration and Terrorism**
  - Infiltration by **terrorists from Pakistan** through the LoC and IB in J&K continues despite fencing and surveillance.
  - **Arms, narcotics, and fake currency** smuggled via Punjab and Rajasthan sectors fuel internal insurgency and organized crime.
  - Recent Example: Drones from across the border dropping weapons in Punjab (2022–24).
- **Illegal Migration and Human Trafficking**
  - **Bangladesh and Nepal borders** witness large-scale undocumented migration, posing demographic, economic, and security threats.
  - **Northeast region** is particularly vulnerable to human trafficking, drug smuggling, and insurgent movement.
- **Lack of Coordinated Border Management**
  - Multiplicity of agencies (BSF, ITBP, Assam Rifles, Army, Customs, State Police) leads to **jurisdictional overlaps and coordination gaps**.

- Absence of a **Unified Border Management Authority** reduces efficiency and accountability.

- **Inadequate Infrastructure**
  - **Poor roads, communication, and outposts** affect quick mobilisation, especially in remote border regions.
  - **Delay in completion** of projects like border fencing, floodlights, and border roads (e.g., along India-China LAC).
  - CAG Reports have flagged delays in completion of border infrastructure projects.
- **Political and Diplomatic Sensitivities**
  - Border disputes (e.g., with China in Eastern Ladakh and Arunachal Pradesh, with Nepal over Kalapani-Limpiyadhura) create **geopolitical instability** and hamper development projects.
  - International relations impact **bilateral mechanisms for border management** (e.g., India-Myanmar insurgent coordination hampered due to junta rule).
- **Socio-Economic and Cultural Linkages**
  - Ethnic and kinship ties across borders (e.g., Nagas in India and Myanmar, Punjabis in India and Pakistan) complicate enforcement of strict border control.
  - Local resistance to fencing and surveillance due to **impact on livelihoods and movement.**
- **Technological and Intelligence Gaps**
  - **Inadequate use of technology** like drones, ground sensors, and smart surveillance.
  - Border guarding forces often lack **real-time intelligence-sharing systems** and analytics-based threat monitoring.
  - **Example:** CIBMS (Comprehensive Integrated Border Management System) still not fully functional across borders.
- **Coastal and Maritime Border Challenges (we will study more about this in next topic)**
  - India's vast coastline faces threats of **arms smuggling, drug trafficking, and infiltration** via fishing boats and cargo vessels.
  - **Example:** 26/11 Mumbai attacks exploited gaps in maritime security.
  - Issues in coordination among **Coast Guard, Navy, Customs, and Marine Police**.

Security Challenges along India's Land Borders

Border with	Major Security Challenges
Pakistan	• Persistent cross-border terrorism and infiltration by groups like Lashkar-e-Taiba and Jaish-e-Mohammed, especially in Jammu & Kashmir. • Frequent ceasefire violations along the Line of Control (LoC), threatening civilian lives and military morale. • Use of drones for smuggling arms, explosives, and narcotics, especially in Punjab. • Narcotics trade and counterfeit currency networks, often routed through Punjab and Rajasthan. • Support to secessionist movements (e.g., revival of Khalistani extremism through ISI funding).
China	• Unresolved boundary disputes, especially in Eastern Ladakh and Arunachal Pradesh (McMahon Line not accepted by China). • Recurrent border transgressions and stand-offs (e.g., 2020 Galwan Valley clash, Tawang face-off in 2022). • Massive infrastructure buildup by PLA close to LAC, shifting status quo. • Information warfare and cyber espionage targeting Indian defence and civilian sectors. • Difficult terrain and weather pose logistical challenges to Indian troop mobility.

Nepal	• Open border exploited for smuggling of arms, narcotics, fake currency, and human trafficking. • Political instability and porous Terai region used as transit routes for illegal activities. • Rising Chinese influence in Nepal poses long-term strategic risks. • Occasional border disputes, such as in Kalapani-Lipulekh region, fuel anti-India sentiments.
Bhutan	• Sanctuary for Indian insurgent groups (e.g., ULFA, NDFB) in dense forests near Assam-Bhutan border. • Smuggling of forest produce, wildlife, and illicit goods. • Strategic concern over Chinese presence near the Doklam tri-junction (2017 standoff). • Terrain makes border policing and surveillance difficult.
Bangladesh	• Illegal immigration leading to demographic imbalances in border states like Assam and West Bengal. • Cattle smuggling and trade in contraband goods (phensedyl, arms, narcotics). • Human trafficking, especially of women and children across the porous border. • Occasional border clashes between BSF and BGB due to enforcement operations. • Difficult riverine terrain hampers full fencing and surveillance.
Myanmar	• Cross-border movement of insurgents from NE India (e.g., NSCN-K, PLA, ULFA) who use Myanmar as safe havens. • Part of the 'Golden Triangle'—a major route for drug trafficking (heroin, meth). • Ethnic kinship across border complicates counter-insurgency and intelligence gathering. • Influx of refugees and arms due to political unrest post-2021 military coup in Myanmar. • Weak border infrastructure and lack of coordinated patrolling with Myanmar Army.

Steps Taken by Government for Effective Border Management

- **Infrastructure Development**
  - **Border Roads Organisation (BRO)**: Constructing all-weather roads in border areas, including the **Strategic Border Roads Project** and projects under **Vibrant Villages Programme** in Arunachal Pradesh, Ladakh, and Uttarakhand.
  - **Fencing and Floodlighting**: Indo-Bangladesh and Indo-Pak borders have been fenced and floodlit under **Border Infrastructure and Management (BIM)** scheme.
    → **3,326 km of fencing completed along the India-Bangladesh border (as of 2024).**
  - **Border Outposts (BOPs)**: Increased construction of BOPs (e.g., BSF, ITBP, SSB) in sensitive stretches.
    → Over **1,400 BOPs operational** along India's international borders.
  - **Forward Airfields and Landing Grounds**: Re-activation and upgradation of advanced landing grounds (ALGs) in Arunachal Pradesh and Ladakh for rapid troop mobilisation.
- **Use of Technology – Smart Borders**
  - **Comprehensive Integrated Border Management System (CIBMS)**: Deployment of smart surveillance using sensors, radars, CCTV, drones, thermal imagers, and satellite data.

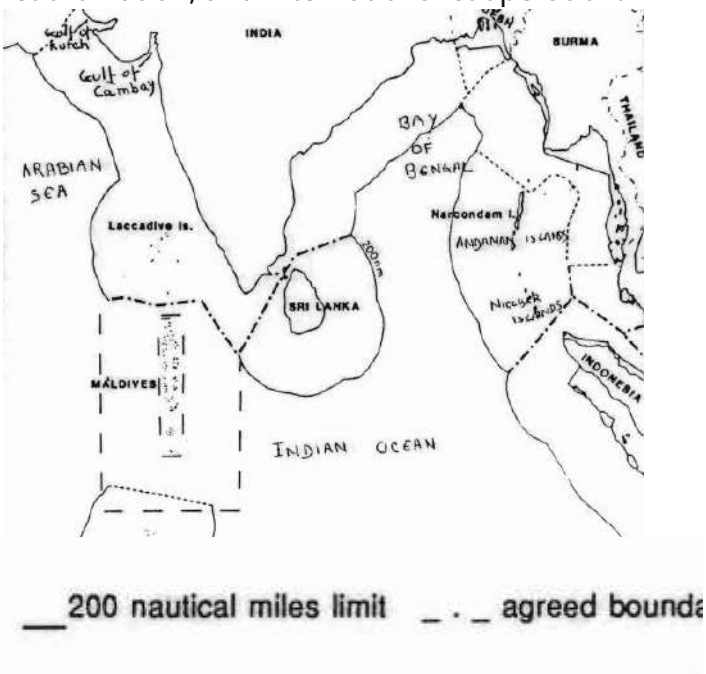
→ Piloted along the Indo-Pak border in the Jammu sector.
    - **Drone Surveillance & Anti-Drone Systems**: Deployed to monitor drug smuggling and arms drops (especially along Punjab-Pakistan border).
    - **Laser Wall and Ground Sensors**: Installed along the LoC and IB to monitor movement in riverine and marshy areas.
    - **Coastal Surveillance Network (CSN)**: Coastal radar chains and Automatic Identification Systems (AIS) for monitoring India's vast coastline.
- **Force Modernisation and Capacity Building**
    - **Modernisation of Police Forces Scheme**: Funds provided to equip border guarding forces with modern weapons, communication tools, and vehicles.
    - **Raising of Special Battalions**: Additional battalions of **ITBP**, **BSF**, and **Assam Rifles** raised to strengthen vulnerable areas.
    - **Special Training Centres**: Jungle warfare, high-altitude warfare, and counter-infiltration training given to border forces.
    - **Youth Recruitment from Border Areas**: Increased representation of local youth in CAPFs to improve intelligence and civil-military relations.
- **Institutional and Administrative Measures**
    - **Unified Command Structures** in sensitive areas like J&K and North East (e.g., Assam Rifles under operational control of Indian Army).
    - **Border Area Development Programme (BADP)**: Funds used to build infrastructure like roads, schools, health centres, and drinking water in border villages.
    - **Vibrant Villages Programme (2022)**: Focused on developing infrastructure and livelihoods in forward areas to check migration and assert territorial presence.
    - **Multi-Agency Centres (MACs)**: Intelligence sharing platforms among IB, RAW, state police, and military intelligence.
- **International Cooperation and Diplomatic Engagement**
    - **Joint Working Groups (JWGs)**: With countries like Bangladesh, Myanmar, Bhutan, and Nepal to coordinate border issues.
    - **Coordinated Border Management Plans (CBMP)**: Especially with Bangladesh to prevent smuggling, illegal migration, and cross-border crime.
    - **Hotlines and Flag Meetings**: Between BSF and BGB (Border Guard Bangladesh), ITBP and Chinese PLA, for incident de-escalation.
    - **Bilateral Border Agreements**: With Myanmar (Operation Sunrise), Bangladesh (Land Boundary Agreement, 2015), Bhutan, and Nepal to regularise border demarcation and management.
- **Legal and Policy Measures**
    - **Citizenship Amendment Act (2019)** and **Foreigners (Tribunals) Order**: For better tracking of illegal migrants.
    - **FCRA Amendments**: To curb the inflow of foreign funds to border-area NGOs that could be misused.

Use of AFSPA (Armed Forces Special Powers Act): In disturbed border areas to give operational freedom to forces during counter-infiltration missions.

2 Maritime Border Management

Introduction

- India's maritime domain is a critical frontier of national security and economic vitality. With a coastline spanning over 7,500 kilometers and an Exclusive Economic Zone of over 2 million square kilometers, the country sits astride major sea lanes in the Indian Ocean—through which nearly 90% of its trade by volume and energy imports flow.
- However, this vast maritime expanse also presents significant security challenges including piracy, smuggling, terrorism, illegal fishing, and growing strategic competition.
- The 26/11 Mumbai attacks exposed the vulnerabilities of India's coastal security, underscoring the urgent need for a robust, multi-layered maritime border management system that integrates surveillance, inter-agency coordination, and international cooperation.



Key Security Challenges along India's Maritime Borders

- **Coastal Terrorism**
  - **2008 Mumbai Attacks** highlighted India's vulnerability to seaborne infiltration.
  - Infiltration of terrorists via fishing trawlers, merchant ships, or unregistered vessels continues to pose a serious threat, especially along porous coastlines like **Gujarat and Maharashtra**.
- **Piracy and Armed Robbery at Sea**
  - Though declining in recent years, incidents in the **Arabian Sea** and **Gulf of Aden** threaten Indian cargo and crew.
  - Increased pirate activity in **Indian Ocean Region (IOR)** affects trade security and maritime logistics.
- **Illegal Migration and Human Trafficking**
  - Maritime routes are increasingly being used for **illegal migration** (e.g., from Tamil Nadu to Sri Lanka or Myanmar).
  - Networks also engage in **human trafficking**, especially across the **Sundarbans** and **Andaman-Nicobar** corridors.
- **Smuggling of Arms, Drugs, and Contraband**
  - Narcotics from the **Golden Crescent (Afghanistan-Pakistan-Iran)** and **Golden Triangle (Myanmar-Laos-Thailand)** enter India via sea routes.
  - **Arms smuggling** from Pakistan or Southeast Asia has been reported in Gujarat and West Bengal coasts.
  - Diesel, gold, and cattle smuggling are prevalent across **India-Bangladesh maritime boundary**.
- **Maritime Boundary Disputes and Intrusions**
  - **Fishermen crossing maritime boundaries** inadvertently lead to arrests and diplomatic friction (notably with Sri Lanka, Bangladesh, and Pakistan).
  - Disputed waters, such as the **Sir Creek** region with Pakistan, remain security-sensitive.
- **China's Naval Expansion and Strategic Presence**
  - **Chinese naval forays** into the IOR, including docking at Hambantota (Sri Lanka) or Gwadar (Pakistan), raise concerns about maritime encirclement or "String of Pearls" strategy.
  - Increasing presence of Chinese surveillance ships and submarines near **Andaman and Nicobar Islands** poses strategic threats.
- **Threats to Critical Maritime Infrastructure**
  - Indian ports (e.g., Mumbai, Kandla, Visakhapatnam) and offshore installations like **ONGC's oil platforms** are vulnerable to sabotage or cyberattacks.
  - Cybersecurity risks to port systems and vessel tracking have increased.

- **Undersea Communication and Energy Infrastructure Security**
  - Vulnerability of **undersea fiber optic cables**, gas pipelines, and transnational marine data systems to sabotage or cyber attacks.
- **Insufficient Coastal Surveillance and Policing**
  - Over **2 lakh small fishing vessels**, many without tracking systems, complicate surveillance.
  - **Lack of coordination** among multiple agencies (Navy, Coast Guard, state police, customs) results in operational gaps.
  - Limited technological infrastructure in **remote islands and coasts** (e.g., Lakshadweep, A&N Islands).

Steps Taken by Government to Secure India's Maritime Border

- **Institutional and Strategic Measures**
  - **National Maritime Security Coordinator (2021):** Appointed under the National Security Council Secretariat (NSCS) to coordinate among Navy, Coast Guard, intelligence, and other maritime stakeholders.
  - **Coastal Security Architecture (Post-26/11):** A 3-tier maritime security framework involving:
    - **Indian Navy** (Blue-water defense)
    - **Indian Coast Guard** (Coastal and EEZ surveillance)
    - **Marine Police/State Forces** (Shallow waters up to 12 nautical miles)
  - **Sagarmala Programme (2015):** While focused on port-led development, it also strengthens port infrastructure and security.
  - **Coastal Security Committees:** At state and district levels, to improve civil-military coordination.
- **Infrastructure and Surveillance Enhancement**
  - **Coastal Radar Chain:**
    - 46 coastal radar stations (Phase-I) already operational.
    - Phase-II expanding coverage to islands and strategic locations like Lakshadweep and A&N Islands.
  - **Automatic Identification Systems (AIS):** Mandatory for large fishing vessels and merchant ships for real-time tracking.
  - **National Command Control Communication and Intelligence (NC3I) Network:** Links Navy, Coast Guard, and marine police for seamless intelligence sharing.
  - **AIS Transponders on Fishing Boats:** Installation on mechanized vessels below 20m length to track coastal activity.
  - **Sagar Suraksha Dal:** Volunteer community watch groups comprising fishermen to report suspicious activities.
- **Capacity Building and Force Deployment**
  - **Indian Coast Guard Expansion:** Increased number of ships, aircraft, hovercrafts, and coastal stations.
    - More than 150 vessels and 60 aircraft operational (2024).
  - **Marine Police Stations:** Established under Coastal Security Scheme (CSS) Phase I & II – over 200 stations in 9 coastal states and 4 UTs.
  - **Joint Coastal Patrolling:** Navy, Coast Guard, and marine police conduct joint exercises for maritime domain awareness.
  - **Offshore Security Coordination Committee (OSCC) :** Headed by DG Coast Guard to safeguard offshore assets like ONGC platforms.
- **Legal and Administrative Frameworks**
  - **Merchant Shipping Act (Amended 2021):** Enhanced penalties for unauthorized movement and lack of tracking systems.
  - **Marine Aids to Navigation Act (2021):** Modernizes lighthouse and coastal navigation safety systems.
  - **Port Security under ISPS Code (International Ship and Port Facility Security Code):** Ensures global standard maritime infrastructure protection.
- **Technology Integration**
  - **Information Management and Analysis Centre (IMAC):** Located in Gurugram, it serves as the nerve center for all maritime data processing.
  - **Maritime Domain Awareness (MDA):** Enabled through integration of radar feeds, satellite imagery, AIS data, and human intelligence.

- **Anti-Drone Systems:** Deployed at high-risk maritime zones and naval installations such as Mumbai, Kochi, Visakhapatnam, and Port Blair, to counter threats from drone-based surveillance or attacks.

- **Community Engagement and Training**
  - **Training of Fishermen:** Coastal communities are sensitized and trained to serve as "eyes and ears" of coastal security.
  - **Issuance of Biometric ID Cards:** Biometric registration of over **20 lakh fishermen** for identity verification and coastal movement monitoring.
  - **Registration and Color Coding of Boats:** Mandatory registration and distinct color codes for state-wise fishing vessels.

Value Addition :

Keywords : Land Border Management, Maritime Border Management, Border Security, Cross-border Infiltration, Terrorism, Illegal Migration, Human Trafficking, Smuggling, Narcotics Trade, Drone Surveillance, Coastal Terrorism, Maritime Piracy, Strategic Infrastructure, Cybersecurity Threats, Maritime Surveillance, Undersea Infrastructure, Border Fencing, Riverine Borders, Porous Borders, Demographic Imbalance, Insurgency, Ethnic Kinship, Territorial Dispute, Maritime Domain Awareness, Smart Borders, Coastal Policing, Illegal Fishing, Arms Trafficking, Strategic Encirclement

Mains Practice Question :

Q1. Discuss the key challenges in managing India's land borders, particularly in the context of terrain diversity and cross-border threats.

Q2. Evaluate the need for a Unified Border Management Authority in India. How can it address the existing institutional fragmentation?

Q3. The 26/11 Mumbai attacks highlighted critical vulnerabilities in India's maritime security. Discuss the post-attack reforms and their effectiveness.

Q4. India's maritime border security requires inter-agency coordination. Examine the structural and operational challenges in achieving this.

In news

Arms training for village along border areas

- Post Operation Sindoor, the Border Security Force has started arms training for village defence guards (VDGs) along the Jammu border with Pakistan. The civilians residing in border villages are being trained as the "second line of defence" in the wake of infiltration by terrorists and terror attacks in Jammu and Kashmir.
- **Border Area Security**
  - Recently ,The Border Security Force got the government's nod to raise 16 more battalions, comprising around 17,000 troopers, and set up two forward headquarters for its western and eastern commands guarding the Pakistan and Bangladesh frontiers, respectively
- **Smuggling along borders**
  - Pakistan continues using Chinese drones to drop narcotics and arms along Punjab border, BSF data shows
- **Comprehensive anti-drone unit to secure its borders**
  - Recently ,Union Home Minister Amit Shahanaounced that, India will soon create a comprehensive anti-drone unit to secure its borders as the "menace" of unmanned aerial vehicles is going to get serious in the coming days.

Acronym

BORDER

(For identifying security challenges in border areas)

- **B – Bootlegging & Smuggling** (Drugs, arms, counterfeit currency)
- **O – Organized Infiltration** (Terrorist crossings, illegal migration)
- **R – Remote Terrain Challenges** (Difficult patrolling, poor infrastructure)

- **D – Demographic Tensions** (Ethnic conflicts, refugee influx)
- **E – External Support to Insurgents**
- **R – Riverine & Maritime Loopholes** (Unmonitored stretches)

SECURE

(For solutions/management strategies)

- **S – Smart Fencing & Surveillance Tech** (Drones, radars, CIBMS)
- **E – Enhanced Border Infrastructure** (Roads, border outposts, telecom)
- **C – Coordination Among Agencies** (BSF, ITBP, Coast Guard, local police)
- **U – Use of Community Engagement** (Border area development, civic action)
- **R – Robust Intelligence Sharing** (Across states and with military)
- **E – Empowering Forces & Reforms** (Better equipment, training, welfare)

FRONTIER

(Comprehensive approach mixing challenges and responses)

- **F – Fencing Gaps & Terrain Obstacles**
- **R – Radical Elements Crossing Over**
- **O – Organized Crime Syndicates**
- **N – Neglect of Local Populations**
- **T – Terror Links to Border Routes**
- **I – Infrastructure Deficit**
- **E – External State Actors' Role**
- **R – Reinforcement Through Modernization**

Ready-Made templates(Intro/Conclusion)

INTRODUCTIONS

- **Strategic Depth:**
  India's borders are not mere geographical lines—they are live faultlines of history, geopolitics, and conflict. From Chinese salami slicing in the north to narco-terrorism in the west, border areas reflect the evolving nature of hybrid threats that challenge sovereignty and stability.
- **Geostrategic Framing:**
  With 15,106 km of land borders and a 7,516 km coastline adjoining hostile and unstable neighbors, India's borders are vulnerable to **cross-border terrorism, smuggling, illegal migration, and proxy warfare**—requiring nuanced and multi-domain management.

- **Integrated Threat Lens:**
  India's border security is complicated by difficult terrain, ethnic linkages across borders, porous boundaries, and state-sponsored threats. Managing these requires synergy between **military preparedness**, **civilian governance**, and **technological modernization**.

- **Contemporary Conflict Insight:**
  Be it the Galwan clash, Rohingya influx, or narco drones in Punjab, the pattern is clear—India's border challenges are now **asymmetric, multi-layered, and politically engineered**, demanding a shift from conventional to intelligent border management.

CONCLUSIONS :

- **Strategic & Developmental Fusion:**
  Securing India's borders demands more than barbed wires—it calls for **smart surveillance**, **border infrastructure**, and **development of border villages** as the first line of national defense. A "whole-of-government" and "whole-of-border" approach is essential.

- **Holistic Security Vision:**
  Border security must balance **force projection** with **people integration**. Ensuring the participation of local communities and aligning security with development is crucial to eliminate both physical and psychological alienation.

- **Future-Oriented:**
  The border of tomorrow will be digital, contested, and psychological. India must invest in **CIBMS, satellite intelligence, AI-based monitoring**, and **bilateral frameworks** to pre-empt threats and project border resilience.

6 UNIT Various Security Forces and Agencies and their Mandate.

Navigating the Syllabus: What You Need to Know

Various Security Forces and Agencies and their Mandate

- Issues Associated with them
- Impact
- Need of Reforms
- Armed forces Reforms
- Reforms in CAPF
- Police Reforms

UPSC Previous year Questions

Question	Nature of Question	Core Demand
Human right activists constantly highlight the view that the Armed Forces (Special Powers) Act, 1958 (AFSPA) is a draconian act leading to cases of human rights abuses by the security forces. What sections of AFSPA are opposed by the activists? Critically evaluate the requirement with reference to the view held by the Apex Court. (2015)	Critical evaluation involving legal provisions, human rights concerns, and judicial interpretation	Identify contentious sections (e.g., Sec. 3, 4, 6); Evaluate necessity vs abuse; Refer Supreme Court views (e.g., 1997 Naga People's case); Balance national security with human rights

Introduction

- India's national security architecture is upheld by a complex ecosystem of armed forces, central police organizations, intelligence agencies, and specialized units—each with a distinct mandate tailored to the country's multifaceted threat landscape.
- From defending borders and combating terrorism to managing internal unrest, cyber threats, and financial crimes, these agencies form the backbone of India's response to security challenges.
- The effective coordination and modernization of these forces are crucial not only for safeguarding sovereignty but also for ensuring internal peace and public trust in state institutions.

Security Forces under Ministry of Defence and Their Challenges

Security Force and its Mandates	Overall Issues Across Army, Navy, and Air Force
Indian Army • Largest component of the armed forces. • Mandated to defend land borders, handle counter-insurgency and internal disturbances. • Operates in diverse terrains: mountains, deserts, forests, and urban conflict zones.	• **Modernization Lag**: Outdated equipment and delayed acquisition of modern arms and technology (e.g., artillery, night-vision, infantry gear). • **Budget Constraints**: High revenue expenditure (~60% of defence budget) leaves limited funds for capital acquisition. • **Shortage of Personnel**: Increasing officer and jawan vacancies; young officers' reluctance to serve in hardship areas.
Indian Navy • Mandated to secure maritime borders, protect maritime trade routes, conduct humanitarian and disaster relief (HADR), and ensure blue-water capabilities. • Plays key role in Indian Ocean Region (IOR) and Indo-Pacific strategy.	• **Inter-Service Coordination**: Absence of true joint command structures hinders integrated operations. • **Dependence on Imports**: ~60% defence equipment is imported, affecting strategic autonomy. • **Cybersecurity & Info Warfare Gaps**: Limited preparedness against new-age threats like cyber warfare, AI-based surveillance, etc.
Indian Air Force (IAF) • Provides air defence of Indian airspace and supports army/navy in joint operations. • Responsible for strategic bombing, surveillance, airlift, and disaster relief. • Plays key role in deterrence and rapid deployment.	

Under Home Ministry CAPF

- Central Armed Police Forces (CAPF) is the collective name of central police organisations in India under the Ministry of Home Affairs (MHA).
- These are technically paramilitary forces formerly known as Central Paramilitary Forces (CPMF).
- Since 2011, India adopted the term "central armed police forces" to drop the word "paramilitary". These forces are responsible for internal security and guarding the borders.

CAPF comprises following central police forces we can study thier mandates and issue associated with these forces in tabular form.

Central Armed Police Forces (CAPFs) and Their Mandates

Name of Force	Mandates / Roles and Responsibilities
1. Central Reserve Police Force (CRPF)	• Main force for **internal security and law & order** across India. • Leads operations against **Left-Wing Extremism (LWE/Naxalism)** under the Ministry of Home Affairs. • Provides **riot control and crowd management** support in civil unrest situations. • Deployed during **elections** for area domination and polling security. • Protects **VIPs**, installations, and sensitive areas through designated battalions. • Hosts elite **COBRA units** for guerrilla warfare in LWE zones. • Engaged in **rescue and disaster response operations**, including during natural calamities.
2. Border Security Force (BSF)	• Guards **India's borders with Pakistan and Bangladesh** in peace time. • Prevents **cross-border infiltration and smuggling** of arms, narcotics, cattle, and human trafficking. • Conducts **anti-tunnel and anti-drone operations** along western borders. • Participates in **counter-insurgency operations**, especially in Jammu & Kashmir and the northeast. • Assists local police during **internal disturbances and communal riots**. • Guards **International Border (IB)** and **coastal areas** (post-2008 Mumbai attacks under coastal security duties)
3. Indo-Tibetan Border Police (ITBP)	• Secures the **3,488 km India-China border (LAC)** in high-altitude, mountainous terrain. • Conducts **patrolling, surveillance, and border outpost management** in inaccessible regions. • Specializes in **high-altitude warfare and disaster response** in the Himalayas. • Coordinates with Army during **standoff situations** like Doklam or Galwan. • Provides **security to vital installations** like the Indian Embassy in Afghanistan (until recently). • Trains troops in **mountaineering, skiing, and survival skills** in extreme cold.
4. Sashastra Seema Bal (SSB)	• Guards **open and friendly borders with Nepal and Bhutan**.

	• Prevents **cross-border smuggling, trafficking, and fake currency movement**. • Promotes **civic action programs** for confidence-building among border communities. • Collects **human intelligence and border population feedback** for strategic inputs. • Undertakes **anti-insurgency operations** in coordination with local police in eastern states. • Supports **disaster relief and rescue** during floods, landslides, and other emergencies.
5. Central Industrial Security Force (CISF)	• Provides **security to strategic installations**, including nuclear power plants, space agencies (ISRO), and oil refineries. • Secures **civil aviation infrastructure**—deploys at over 60 airports across India. • Protects **Delhi Metro, PSUs, and government buildings** such as Parliament House. • Offers **security consultancy** to private industries and VIPs on request. • Manages **Quick Reaction Teams (QRTs)** in urban areas for counter-terror response. • Provides **fire safety and disaster management support** in high-risk industrial areas
6. Assam Rifles	• Oldest paramilitary force, deployed primarily in **northeast India**. • Conducts **counter-insurgency and counter-terrorism operations** under Army's operational control. • Guards the **India–Myanmar border**, preventing smuggling and illegal migration. • Carries out **civic action programs** to win hearts and minds in insurgency-prone areas. • Assists in **infrastructure development and welfare activities** in remote tribal areas. • Plays a crucial role in **intelligence gathering** and surveillance in border regions.

Issues Associated with Central Armed Police Forces (CAPFs)

- **Operational Stress and Deployment Fatigue**
  - CAPFs, especially CRPF and BSF, are deployed continuously in high-risk areas like Jammu & Kashmir, Left-Wing Extremism (LWE)-affected districts, and riot-prone regions without adequate rest or rotation. This leads to physical exhaustion and psychological distress.
  - Cases of **suicides and fratricide** among personnel have increased in recent years due to operational stress and lack of leave.
  - Many units operate without a proper **peace-posting cycle**, unlike the Army's rest-deployment rotation model.
- **Human Resource and Welfare Challenges**
  - There is a significant number of **vacant posts** in several CAPFs, especially among officers and specialized units like COBRA.
  - **Poor living conditions** at forward posts—lack of sanitation, water, internet access, and

medical facilities—impact the morale of jawans.
    - **Limited career growth** and stagnation in promotions for directly recruited CAPF personnel, especially when key leadership posts are filled by deputed IPS officers.
    - **Disparity in pay and pension benefits** compared to the Armed Forces, despite similar or even harsher service conditions.
- **Training and Skill Gaps**
    - Most CAPFs lack access to **modern training modules** for urban warfare, cyber threats, drone countermeasures, or AI-based surveillance.
    - There is insufficient **joint training or inter-agency exercises** between CAPFs and state police or the military, which leads to poor coordination during real-time operations.
    - Many personnel are still trained using **obsolete tactics and outdated equipment**.
- **Inadequate Equipment and Modernization**
    - There are severe shortages in essential combat gear such as **bulletproof jackets, mine-protected vehicles, surveillance drones**, and modern firearms.
    - CAPFs deployed in border areas like the ITBP or SSB face logistical constraints due to **poor infrastructure**, lack of all-weather roads, and unreliable communication networks.
    - Despite announcements under the **Police Modernisation Scheme**, actual procurement is slow and bureaucratically delayed.
- **Organizational and Structural Issues**
    - There is **overlapping jurisdiction and ambiguity** among CAPFs and between CAPFs and state police, especially in counter-insurgency zones.
    - **Coordination failures** arise due to the absence of an integrated command structure; for example, the dual control over Assam Rifles (MHA for admin, Army for ops) creates functional confusion.
    - **No unified internal security doctrine**, unlike the Armed Forces which operate under a centralized defence policy.
- **Leadership and Institutional Weakness**
    - Key leadership roles in CAPFs are usually occupied by **IPS officers on deputation**, which leads to dissatisfaction among career CAPF officers.
    - Frequent transfers, lack of long-term command tenures, and politicization of postings dilute leadership effectiveness.
    - There is also a **disconnect between policy-makers and ground realities**, with few reforms implemented from committee recommendations (e.g., Madhukar Gupta Committee on border management).

Joshi Committee Recommendations for CAPF

- **Cadre Management**: Top positions in CAPFs should be filled from within the respective cadres to boost morale and ensure career progression. Regular cadre reviews should be conducted within a defined timeline.
- **Training Enhancements**: Update training curricula to include modern technologies such as Information Technology, cybersecurity, and cybercrime. Ensure that training infrastructure is adequately equipped.
- **Modernization Efforts**: Streamline procurement processes to avoid delays. Engage with ordnance factories and private manufacturers to ensure a steady supply of equipment.
- **State Police Capacity Building**: Encourage states to develop their own police forces for routine law and order duties, reducing over-reliance on CAPFs. The central government should support states through financial assistance and training.
- **Housing and Welfare**: Address the shortfall in housing for CAPF personnel by collaborating with state governments to allocate land and resources.
- **Intelligence Gathering**: Strengthen intelligence mechanisms with better coordination among agencies and autonomy in personnel recruitment.

Intelligence and Investigative Agencies and Their Mandates

Name of the Agency	Mandate / Roles and Responsibilities
Intelligence Bureau (IB)	• India's premier **internal intelligence agency** under the Ministry of Home Affairs (MHA). • Responsible for gathering and analyzing intelligence related to **internal threats**, including terrorism, insurgency, espionage, and communal unrest. • Coordinates with state police and security forces for **preventive intelligence**. • Monitors political movements, extremist groups, and anti-national activities within the country. • Plays a key role in **VIP security and counter-radicalization efforts**.
Research and Analysis Wing (R&AW)	• India's **external intelligence agency** under the Cabinet Secretariat. • Focuses on gathering strategic and foreign intelligence relating to **India's external security threats**. • Monitors **military, political, and economic developments** in neighboring countries and regions of interest. • Plays a role in **covert operations and foreign counterintelligence**. • Works closely with Indian missions abroad and international intelligence partners.
National Investigation Agency (NIA)	• India's **counter-terrorism investigative agency**, formed under the NIA Act, 2008. • Investigates and prosecutes **offenses affecting national security**, especially those listed in the Schedule of the NIA Act (e.g., UAPA, Explosives Act, etc.). • Handles cases related to **terror funding, organized crime, and cross-border terrorism**. • Has jurisdiction across the country and can take over cases from state police after MHA approval. • Strengthening cooperation with state ATS and central forces like NSG.
Central Bureau of Investigation (CBI)	• India's premier **investigative agency**, functioning under the Department of Personnel and Training (DoPT). • Investigates **high-profile criminal cases**, including corruption, financial fraud, economic offenses, and special crimes. • Handles cases referred by **Central Government, State Governments, or courts (e.g., Supreme Court, High Courts)**. • Divided into divisions like Anti-Corruption, Economic Offenses, and Special Crimes. • Works in coordination with Interpol for international investigations.

State Police Forces

Common Mandates of State Police Forces	Common Challenges Faced by State Police Forces
• **Maintenance of law and order** across urban and rural areas. • **Crime prevention and detection**, including investigation of cognizable and non-cognizable offenses. • **Traffic management** and road safety enforcement. • **Management of public protests, rallies, and crowd control** during festivals and elections. • **Implementation of state and central laws** and execution of court orders. • **Maintaining communal harmony and preventing caste- or religion-based violence**. • **Coordination with central agencies** (e.g., NIA, IB, CBI) in matters of national security, terrorism, and organized crime. • **Collection of local intelligence** on potential security threats, communal tensions, or criminal activities.	• **Political interference** in appointments, postings, and investigations. • **Inadequate manpower and poor police-population ratio** (India's average is ~152 per lakh population; UN norm is 222). • **Lack of modern equipment**, forensic labs, and cybercrime capabilities. • **Poor training and capacity building**, especially in handling new-age crimes like cyber fraud, financial crimes, and social media misuse. • **Stress and overwork**, leading to low morale, high attrition, and increasing cases of suicides/fratricides. • **Low conviction rates** due to weak investigations, procedural delays, and poor evidence collection. • **Lack of public trust**, especially in cases of custodial deaths, excessive use of force, and police brutality. • **Outdated colonial laws** like the Police Act of 1861 still govern most state police operations.

Various Committees and Recommendations For Police Reforms

1. Padmanabhaih Committee on Police Reforms

- Separate investigation from law and order duties.
- Establish mechanisms for police accountability.
- Enhance police training and capacity building.
- Promote community policing for better engagement with the public.
- Utilize technology for improved police operations and investigations.

2. In Prakash Singh case in 2006 SC gave following Directives on Police Reforms

- Constitute a state security commission to make sure that the state does not exercise undue influence on the police.
- The DGP should be appointed through a transparent and merit-based process and have a minimum tenure of two years.
- Set up a National security commission at the Central level.
- Set up police complete authority at state and district level.
- Set up a Police establishment board.

3. NITI Aayog suggested the following reforms

- States should be encouraged, with fiscal incentives, to introduce 'The Model Police Act of 2015' as it modernizes the mandate of the police.
- A Task Force must be created under the MHA to identify non-core functions that can be outsourced to save on manpower and help in reducing the workload of the police.
- The states should be encouraged to ensure that the representation of women in the police force is increased.
- Moving police as well as public order to the Concurrent List to tackle increasing inter-state crime and terrorism under a unified framework.

Value Addition

In news

- **SC Judgement**
  - Recently, The Supreme Court ruled that Group A officers of the Central Armed Police Force (CAPF) from batches dating back to 1986 are recognised as "Organised Services" for "all purposes".
- **Ministry of Home Affairs data**
  - Over 50,000 Central Armed Police Force (CAPF) personnel quit jobs in the past five years, according to data provided by the Ministry of Home Affairs (MHA) to a parliamentary panel. The highest attrition was in 2022, when 11,884 personnel quit services.
- **IPS Posting in CAPF**
  - Recently ,In a landmark order, the Supreme Court has directed that the deputation of IPS officers up to the inspector general rank in the CAPFs should be "progressively reduced" over two years to give more opportunities to cadre officers.

Acronym

STRIFE – Issues Faced by Security Forces and Agencies

- **S – Shortage of Manpower & Modern Equipment**: Many forces operate with outdated technology and understaffing
- **T – Training Gaps**: Limited exposure to modern warfare, cyber threats, and tech-enabled crime
- **R – Role Overlaps & Jurisdictional Conflicts**: Multiple agencies with similar mandates create confusion and inefficiencies
- **I – Inter-Agency Coordination Deficits**: Poor synergy between intelligence, police, and paramilitary units
- **F – Fatigue & Mental Stress**: Long postings, hostile conditions, lack of rest and support systems
- **E – External Pressures & Political Interference**: Impacting operational autonomy and morale

Ready templates on common themes

Cumulative Challenges to security forces

Heading	Subheadings
Political	• Terrorism • Insurgency • Political affiliations
Economic	• Lack of funds • Infrastructure
Social	• Communal tensions • Pressure group
Technological	• Cyber threats • Speed of tech evolution
Geographical	• Porous borders • Difficult terrain • Climate

PRAYAAS

PRAYAAS EDUCATION ™

CTS NO 1262/B Plot No. 594B,
Office 301A, 301 2nd floor Starling Plaza,
J M Road, Pune, +91 7378743031