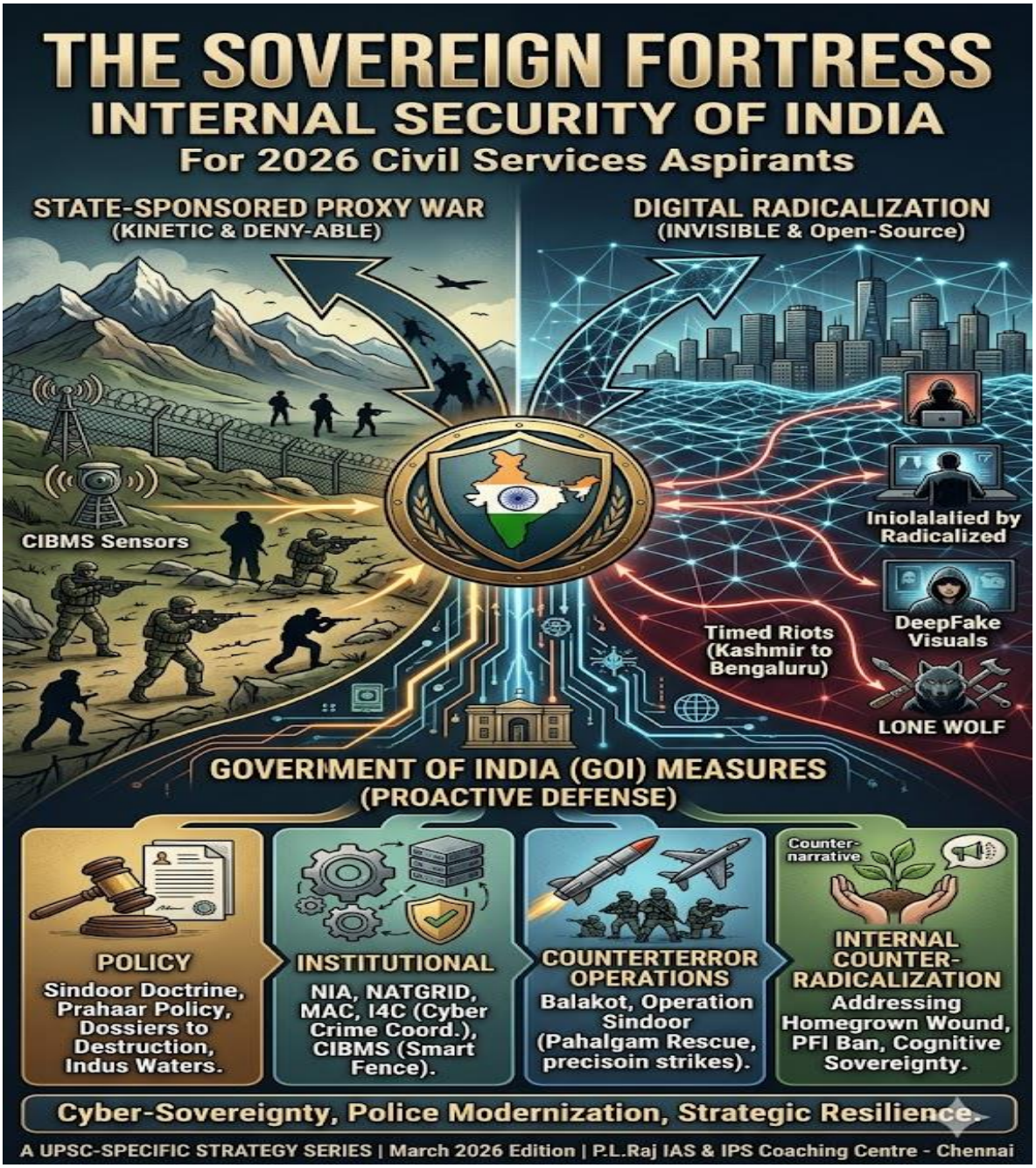

THE SOVEREIGN FORTRESS
INTERNAL SECURITY OF INDIA
For 2026 Civil Services Aspirants
STATE-SPONSORED PROXY WAR
(KINETIC & DENY-ABLE)
DIGITAL RADICALIZATION
(INVISIBLE & Open-Source)
CIBMS Sensors
Iniolalalied by Radicalized
DeepFake Visuals
Timed Riots (Kashmir to Bengaluru)
LONE WOLF
GOVERIMENT OF INDIA (GOI) MEASURES
(PROACTIVE DEFENSE)
POLICY
Sindoor Doctrine, Prahaar Policy, Dossiers to Destruction, Indus Waters.
INSTITUTIONAL
NIA, NATGRID, MAC, I4C (Cyber Crime Coord.), CIBMS (Smart Fence).
COUNTERTERROR OPERATIONS
Balakot, Operation Sindoor (Pahalgam Rescue, precisoin strikes).
Counter-narrative
INTERNAL COUNTER-RADICALIZATION
Addressing Homegrown Wound, PFI Ban, Cognitive Sovereignty.
Cyber-Sovereignty, Police Modernization, Strategic Resilience.
A UPSC-SPECIFIC STRATEGY SERIES | March 2026 Edition | P.L.Raj IAS & IPS Coaching Centre - Chennai

THE SOVEREIGN FORTRESS

Internal Security of India

A Comprehensive Guide for 2026 Civil Services Aspirants

Mastering the "Shadow War": From Policy to Praxis

- **Integrated Border Management**
- **The Cyber-Physical Frontier**
- **Dismantling the Crime-Terror Nexus**
- **The New Legal Architecture (BNS & DPDP)**

By M.R. Sridhar Radha Krishnan for P.L. Raj IAS Chennai

P.L.Raj IAS & IPS Coaching Centre – Chennai

March 2026 Edition

Introduction

For the 2026 civil services aspirant, the journey through India's internal security is a journey into the heart of a nation finally waking up. For decades, we were a "Soft State"—a country that lived by the "Chalta Hai" (casual) attitude, waiting for a tragedy to strike before we even looked at our files.

We admitted the "Homegrown Wounds" of Naxalism, the "Shadow War" in Kashmir, and the "Digital Poison" of cyber-attacks to fester because our elite in Delhi were too comfortable.

But the India of 2026 is different. The "Red Corridor" is no longer a bleeding line; it is a series of shrinking dots on a map. The "Sea-Blindness" that led to 26/11 attack has been replaced by a digital wall of radars and drones. We have moved from a nation that "managed" its problems into a nation that "eliminates" them.

The new laws—the **BNS** and the **DPDP Act**—and the high-tech eyes of **NATGRID** are not just bureaucratic tools. They are the new nervous system of a Republic that has decided to be a Sovereign Power, not a victim.

Contents

Unit-1:

Internal Security – Framework and Dynamics

Definition of Internal Security

Internal Security refers to the maintenance of peace, law and order, and the sovereignty of the State within its national boundaries.

- **Constitutional Basis:** Under **Article 355**, it is the duty of the Union to protect every State against external aggression and **internal disturbance**.
- **Distinction:** Unlike 'External Security' (managed by the Ministry of Defence), 'Internal Security' is primarily the mandate of the **Ministry of Home Affairs (MHA)** and involves the coordination of State Police and Central Armed Police Forces (CAPFs).

Significance of Internal Security

The maintenance of internal stability is essential for the following reasons:

1. **Economic Growth:** Ensures a stable environment for investment, infrastructure development, and the "Viksit Bharat" 2047 goals.
2. **National Integrity:** Prevents secessionist and anti-national tendencies that threaten the federal structure.
3. **Social Harmony:** Safeguards the secular and pluralistic structure of Indian society from communal or ethnic violence.
4. **Democratic Continuity:** Allows for the free and fair elections and the impartial functioning of constitutional bodies.

Major Objectives

The primary objectives of the Indian Internal Security apparatus are:

- **Maintenance of Rule of Law:** Ensuring the primacy of the legal system and the protection of civil liberties.
- **Neutralizing Subversive Elements:** Addressing threats from insurgents (LWE), terrorists (Proxy wars), and secessionists.
- **Protection of Critical Infrastructure:** Securing power grids, financial hubs, and digital networks (Cyber security).
- **Human Security:** Mitigating non-traditional threats like drug trafficking (Narco-terrorism) and organized crime.

The Distinctive feature of India's internal security threats.

- What makes India's situation unique? It is the **"Internal-External Blur."**
- Most countries face either an external invasion or a domestic revolt. India faces a permanent "Proxy War." We have a nuclear-armed neighbour that uses internal fault lines—be it caste, religion, or language—to destabilize the centre. No other democracy in the world manages such a vast, diverse population while simultaneously being targeted by state-sponsored cross-border terrorism.
- Furthermore, our challenges are distinct because we are trying to solve 19th-century land disputes and 20th-century ideological wars with 21st-century technology—all while staying a committed democracy.

Evolution of Internal Security challenges -

The internal security challenges have evolved through four distinct historical phases:

No	Phase	Period	Primary threat Focus
1	**Phase I**	1947 – 1960s	Post-Partition integration, Princely State issues, and early North-East ethnic assertions.
2	**Phase II**	1960s – 1980s	Rise of the Naxalite movement (1967) and Punjab militancy. Focus on ideological and ethnic insurgencies.
3	**Phase III**	1990s – 2010s	Cross-border terrorism in J&K, rise of Proxy War, and the emergence of the "Red Corridor" (LWE).

4	**Phase IV**	2020 – Present	**Hybrid Warfare:** Cyber-warfare, radicalization via social media, Drones/UAVs, and "Grey Zone" tactics.

Internal Security management focus

A. The Mission (Short-Term: Target 2026)

The current mission is characterized by a "Zero Tolerance Policy" toward terrorism and extremism.

1. **LWE Elimination:** A dedicated mission to completely eradicate Left Wing Extremism by **2026** through the **SAMADHAN** strategy.
2. **North-East Normalcy:** Consolidating peace through various Accords (e.g., Bodo, Karbi Anglong, ULFA peace deals) and the phased reduction of **AFSPA**.
3. **Institutional Strengthening:** Enhancing the capabilities of the NIA (National Investigation Agency) and NATGRID.

B. The Vision (Long-Term: Towards 2047)

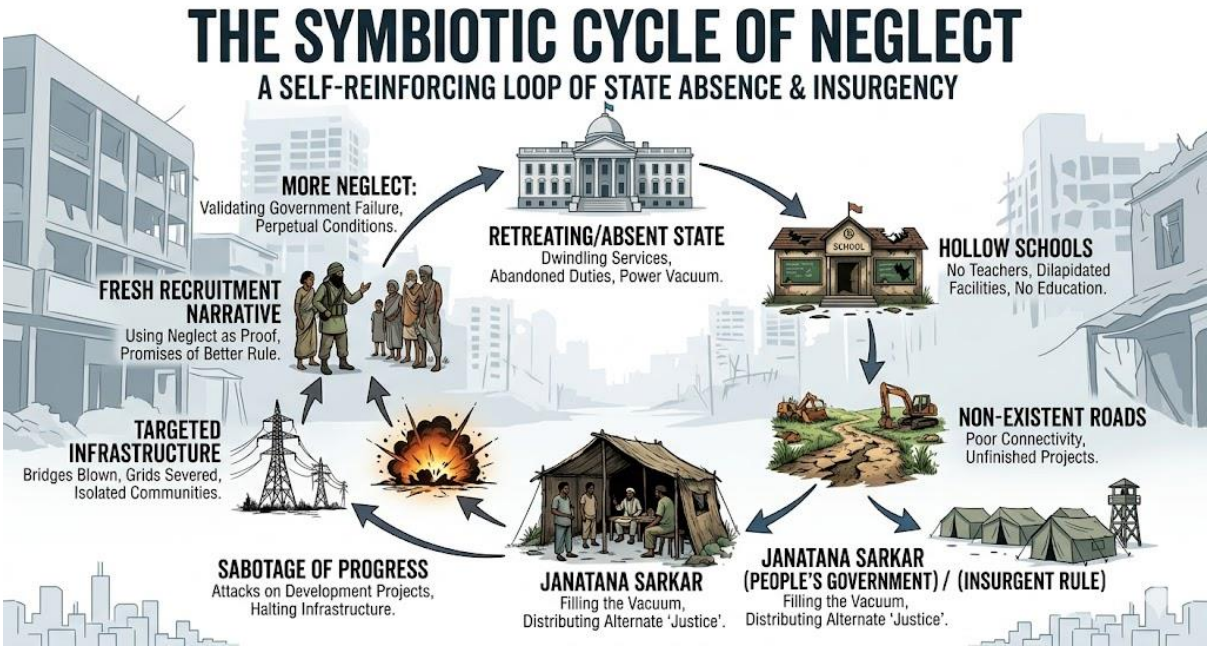
The vision for 2026 and beyond focuses on a "Technology-Sovereign" security architecture:

1. **Surakshit Bharat:** Transitioning from reactive policing to **proactive/predictive policing** using AI and Big Data.
2. **Cyber-Physical Security:** Integrating the **National Cyber Security Strategy** with physical border management (CIBMS).
3. **Community Resilience:** Building a "Perception Management" framework to deny local support to extremist ideologies.

Unit -2

Development Problem and Spread of Extremism - linkage

I. The Linkages: The Symbiotic Cycle of Neglect



The relationship between development and extremism is not merely linear; it is **circular and self-reinforcing**.

- **The Breeding Ground:** Extremism thrives in the vacuum left by a retreating or absent state. Where schools are hollow shells and roads are non-existent, the "Janatana Sarkar" (People's Government) of the Maoists steps in to it and provide a arbritrary—and violent—form of order.
- **The Sabotage of Progress:** Ironically, LWE then targets the very infrastructure needed for development (schools, telecom towers, railways), branding them as tools of "state penetration." This keeps the region in a state of **perpetual backwardness of the communities**, which the insurgents then use them for a fresh recruitment drive.

- **The 2026 Shift:** Presently we are able to transform the **"Red Corridor"** into **"Growth Corridors."** The current strategy recognizes that security can "clear" an area, but only development can "hold" it.

The Fundamental Reasons for the threat to Internal Security.

- Why is India so uniquely plagued? The answer is, the same core rot: **The Developmental and Governance Deficit.**
- The fundamental reason for all our challenges is the absence of the "Rule of Law" in the last mile. When the district administration fails, the insurgent steps in. When the police are seen as a feudal tool of the powerful rather than a protector of the citizen, people look for alternatives. Extremism thrives in the vacuum left by a state that is often heavy-handed at the central level but invisible at the village level.

The Development Deficit: The Basic Cause of Frustration

A development deficit is the primary trigger for extremism because it creates a sense of **Relative Deprivation**.

1. **Structural Dispossession:** Historically, the colonial era Land Acquisition and Forest policies alienated the tribal communities from their "Jal, Jangal, Jameen" (Water, Forest, Land). But , the continuity of the same patterns in the post-colonial times, created a pool of "historical grievances."
2. **The Governance Vacuum:** The deficit is not only about a lack of money, but a **lack of presence**. When the "Rule of Law" is invisible, the "Rule of the Gun" becomes the only arbiter.
3. **Aspiration vs. Reality:** In a digital age, even the most remote tribal youth can see the prosperity of urban India through a smartphone. When this aspiration meets a lack of local schools and jobs, the resulting frustration is easily infected by Maoist ideologues.

The 2026 Development Model: A Roadmap for Stability

To prohibit frustration and extremism, the state has adopted a **Saturation Model**—moving from "selective intervention" to "universal entitlement."

- **The Dharti Aaba Janjatiya Gram Utkarsh Abhiyan (2024-2026):** This is the flagship 2026 model. It aims for **100% saturation** of 17 interventions (housing, water, electricity, and health) in over 63,000 tribal-dominated villages. It seeks to leave "zero vacuum" for extremist propaganda.
- **The Aspirational Districts & Blocks Program:** By using "Delta Rankings," the state creates a competitive spirit among local administrations to improve Human Development Index (HDI) markers.
- **Economic Sovereignty with autonomy:** Strengthening the **Panchayats (Extension to Scheduled Areas) Act (PESA)** and the **Forest Rights Act (FRA)** to give tribes legal control over Minor Forest Produce (MFP), ensuring that development is not "imposed" but "owned."

Way Forward: Toward a Naxal-Free Republic

As we enter the final phase of LWE elimination by 2026, the way forward involves three critical pillars:

1. **Cognitive Sovereignty:** Countering the Maoist information warfare by showcasing the success of the "surrender and rehabilitation" policies. The state must win the "War of Narratives" on social media.
2. **Last-Mile Connectivity:** Completing the **Road Requirement Plan (RRP)** and the **4G Saturation Plan** in the deep interiors of Abujhmad to ensure that the district administration is only a few minutes—not days—away from any citizen.
3. **Institutional Resilience:** Moving from a "Central Armed Police Force (CAPF) lead" to a **"State Police lead"** in security, ensuring that the local police stations become the permanent anchors of development and grievance redressal.

Conclusion

The "final blow" against LWE in 2026 is not being delivered by the barrel of a gun, but by the construction of a bridge and the opening of a bank branch. The **March 2026 target** is not just a security deadline; it is a promise of integration. For the Indian Republic, the elimination of extremism is the ultimate validation of its democratic model—proving that development, when delivered with justice and intent, can defeat even the most entrenched of violent ideologies.

Unit -3

External State and Non State actors

Defining the Players: The Sovereign and the Shadow

- **State Actors:** These are the formal institutions of a sovereign country. When we speak of threats to India, we are talking about the **ISI (Inter-Services Intelligence)** of Pakistan or the **PLA (People's Liberation Army)** of China. They have budgets, embassies, and a seat at the UN. Their menace is institutional.
-
- **Non-State Actors (NSAs):** These are individuals or groups that function independently of any state authority. This includes the **LeT (Lashkar-e-Taiba)**, the **Maoists** in our forests, or the **Cyber-syndicates** operating from the Dark Web. They have no flag, no accountability, and no "official" address. Their menace is informally institutional.
-

The Great Delusion: Differences and Similarities

To understand the 2026 security matrix, one must see through the "Plausible Deniability" that perfected by globalization.

There exist a superficial differences between them but a lethal coordination and similarity in terror act.

1. The Superficial Differences

- **Legitimacy:** State actors claim the "divine right" of sovereignty. Non-state actors are, by definition, outlaws.
- **Resources:** A state has a central bank; a non-state actor has a narcotics pipeline or a "protection tax" from a village.
- **Accountability:** If a state actor strikes, it risks a formal war. If a non-state actor strikes, the state sponsor simply shrugs and points to "rogue elements."

2. The Lethal Similarities

- **The Objective:** Both seek to erode the **Indian State's authority**. Whether it's a Chinese cyber-attack on our power grid or a Naxalite IED in Bastar, the goal is to prove the Indian State is weak.
- **The Tools:** Both use the same encrypted apps, the same high-grade "off-the-shelf" drones, and the same digital propaganda to radicalize.
- **The "State-Sponsored" Hybrid:** This is the most critical concept. In our neighborhood, the Non-State Actor is often merely a **"sub-unit"** of the State. The LeT does not move a finger without the ISI's nod. They are "Proxies"—the State's "dirty hands."

Its impact on India: A Republic under Siege

India's unique geography—stuck between a nuclear-armed state sponsor of terror and a global superpower with expansionist aims—creates a specific set of implications.

1. **The 'Two-Front' Paradox:** We are forced to spend billions on conventional weapons (Rafales, Tanks) to deter the **State Actor**, while our soldiers are being killed by the **Non-State Actor's** 50-rupee IED. It is a massive drain on our "Viksit Bharat" exchequer.
2. **Exploiting Democracy:** These actors use India's own freedoms against it. They use our free press to spread panic and our slow judicial system to protect their "over ground workers."
3. **The Perception War:** By using non-state actors, our adversaries ensure India is seen as "unstable." This scares away the very foreign investment we need for our economic leap.

The Organized Menace: The Terror-Crime Nexus

The most alarming development for 2026 is the **"Corporate"** nature of this menace. It is no longer about "ideology"; it is about **"The Business of Chaos."**

- **Narco-Terrorism:** The "Golden Crescent" drugs are sold in Punjab to fund the "Proxy War" in Kashmir. The Non-State Actor is the distributor, while the State Actor provides the "safe passage" through the border.
- **Money Laundering:** The proceeds of crime are "layered" through global shell companies—a feat only possible because certain State Actors provide "tax havens" and financial anonymity.
- **Cyber-Mercenaries:** We now see state-backed groups (like the Lazarus group or Chinese APTs) hiring non-state hackers to do their terror work. It is an **"Uber-model"** of terrorism.

- **The Insurgent-Criminal Alliance:** The **Maoist and Naxal** movements have mutated from forest ideologues into high-end protection rackets, providing logistics for organized crime in exchange for sophisticated weaponry.
- **Illegal migrants** are no longer just a demographic concern; they have become the perfect, untraceable "sleeper" infrastructure for infiltrating agents and smuggling arms across porous frontiers.

The Concerns

The real concern isn't that these actors exist—they always have. The concern is the **"Governance Lag."**

- **The Intelligence Deficit:** Our agencies are still playing catch-up with encrypted "lone wolf" communications.
- **The Legal Maze:** Our laws (UAPA, PMLA) are often bogged down in procedural delays, while the adversary moves at the speed of light.
- **The Strategic Silence:** For too long, India's response has been reactive. We wait for the "Non-State" strike and then complain to the "State" sponsor.

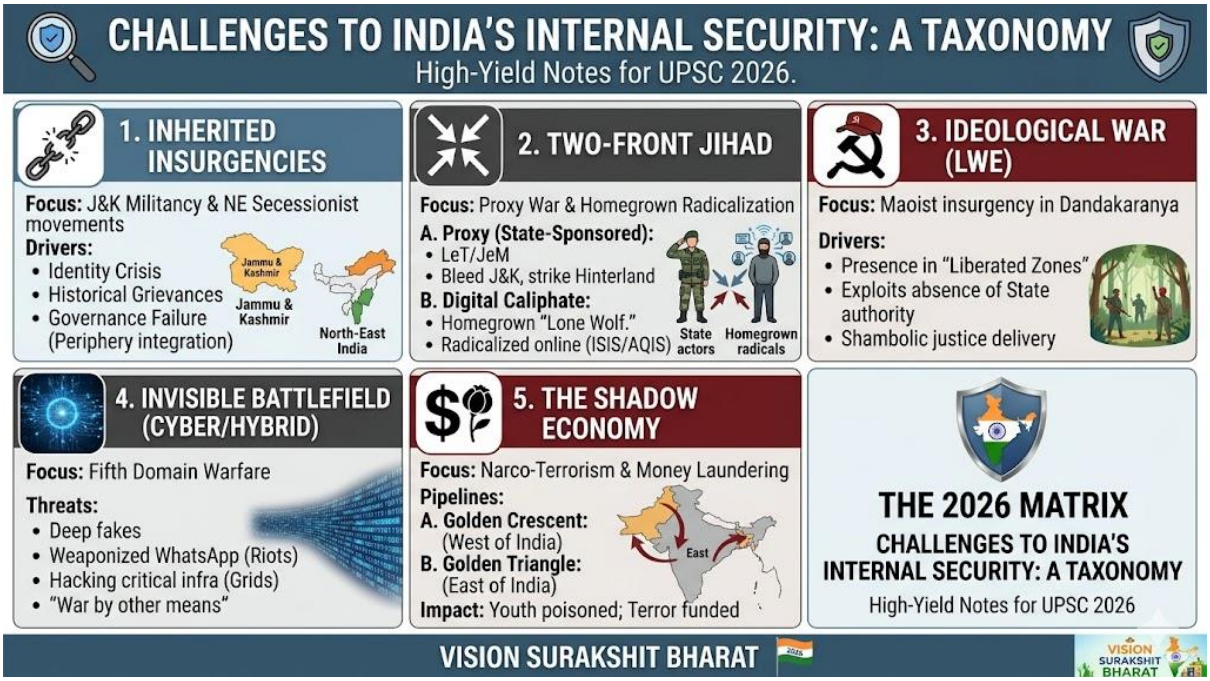
Final Insight:

In your Mains answer, dont use the phrase "innocent civilians misled." Call them what they are: **"Fifth Columnists"** and **"Strategic Proxies."** Argue that the only way to defeat the Non-State Actor is to make the cost of sponsorship unbearable for the State Actor. Internal security is won not in the courtroom, but by asserting the **uncompromising sovereignty** of the Indian State.

Unit -4

Types of Internal Security Challenges

While studying textually, we often categorize the threats into neat boxes. But on the ground, these threats are messy and overlapping. We can broadly divide them into:



1. **The Inherited Insurgencies:** These are the **"decadal bleeding of India"** —the secessionist movements in the **North-East** and the lingering shadow of militancy in **Jammu & Kashmir**. They are fueled by identity, historical grievances, and, frankly, the failure of the State to integrate the periphery into the heartland

2. The Two-Front war

In India, this isn't a monolith; it's a Pan Islamic terror movement that has evolved significantly since the 1990s.

i. **The Proxy War (State-Sponsored):** This is the old, brutal reality of groups like Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM). They are the "auxiliary sub-units" of a neighbour's military strategy. Their goal is simple: to keep India bleeding in Kashmir and occasionally strike the "hinterland" (Mumbai, Delhi) to shatter investor confidence.

ii. **The Digital Caliphate (Home-grown Radicalization):** This is the newer, more insidious threat. It's the shift from organized cells (like the old SIMI or Indian Mujahideen) to **"Lone Wolf"** actors. These are individuals radicalized entirely online, often by global entities like ISIS or Al-Qaeda in the Indian Subcontinent (AQIS), who use local grievances to spark global-scale violence.

2. **The Ideological War:** Left-Wing Extremism (LWE). It is a war fought in the "liberated zones" of the Dandakaranya forest, where the state merely present, and the Maoist is the only provider of a shambolic form of justice.
3. **The Invisible Battlefield (Cyber & Hybrid):** This is where the 2026 aspirant must focus. It is the war of deep fakes, the weaponization of WhatsApp, Face Book and through other social media to spark a riot in minutes, and the hacking of power grids. It is "war by other means."
4. **The Shadow Economy:** Narco-terrorism and money laundering. The "Golden Crescent" and "Golden Triangle" aren't just names on a map; they are the pipelines through which the youth are poisoned and terror is funded.

The Priority of threats.

If you ask the Home Ministry, every threat is a priority. But for a nation with limited resources, we must choose.

- **Immediate Priority: Cyber & Information Warfare.** Why? Because it is pervasive. A bomb affects a street; a manipulated narrative on social media can burn a whole state. The ability of external actors to radicalize a youth in a small town via a screen is the most potent threat today.
- **The Strategic Exit: Left-Wing Extremism.** With the 2026 goal for its elimination, the priority here is "The Final Push"—not just through boots on the ground, but through the "SAMADHAN" framework of roads, schools, and banks.
- **The Constant Vigil: Border Management.** As long as we have a neighbor that uses terror as state policy, the security of our land and maritime frontiers remains an existential priority.

The impact of Globalization on Internal security threat.

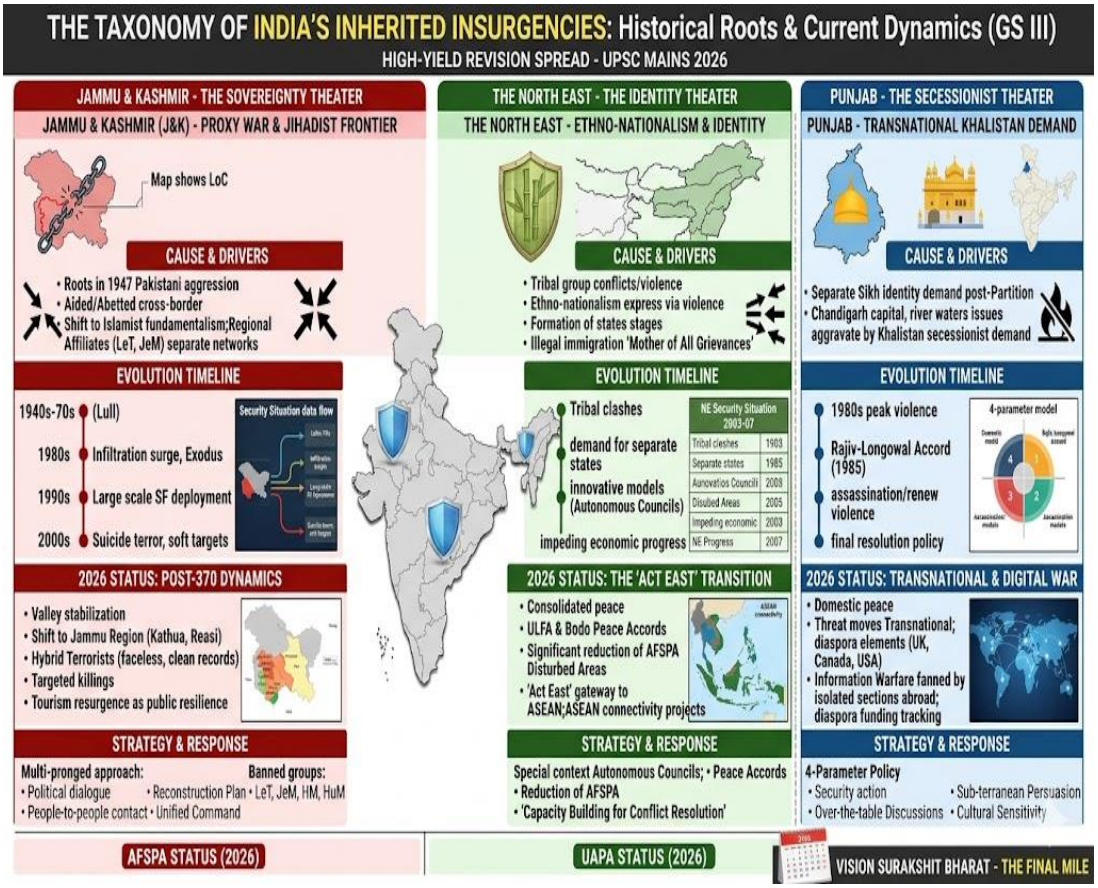
Globalization was supposed to be about the free flow of goods and ideas. For India's internal security, it has been a double-edged sword.

1. **The Porosity of the Digital Border:** Globalization has made borders irrelevant for the "keyboard mujahedeen." Radicalization is now outsourced to the cloud.
2. **The Finance of Fear:** Money can be "layered" through shell companies across continents in seconds. Terrorists now use Crypto currency, making the task of the Enforcement Directorate (ED) a digital nightmare.
3. **The Transnational Nexus:** An insurgent in Nagaland can now source arms from Southeast Asia and find sanctuary in Myanmar, all while coordinating via encrypted apps developed in Silicon Valley.

Unit -5

The Internal Security Threats

Inherited Insurgencies



Defining the 'Inherited Insurgency'(Decadal Terrorism)

An **Inherited Insurgency** refers to those armed internal conflicts that are rooted in the very birth of the Indian Republic. Unlike modern "lone wolf" attacks or cyber-terror, these are structural challenges involving territory, ethnic identity, and sovereignty. They are "inherited" because they stem from historical grievances—often colonial or post-Partition—that have evolved through decades of Cold War geopolitics and, more recently, global religious radicalization.

The Triad of Conflict

India's internal security landscape is historically defined by three distinct geographic and ideological driven terror theatres:

1. **The Sovereignty Theatre:** Jammu & Kashmir (Cross-border proxy war).
2. **The Ethno Identity Theatre:** The North Eastern States (Ethno-nationalism).
3. **The Religious - Cultural Theatre:** Punjab (Secessionist embers).

Jammu & Kashmir: The Long Shadow of 1947

In J&K, the insurgency is not a local uprising but a sophisticated proxy war that has mutated from a territorial dispute into a **Global Jihadist frontier**.

Evolution of the Conflict

- **The Genesis (1947-1971):** The root lies in Pakistan's initial attempt to capture the state by force in 1947. Post-1971, there was a temporary "lull" as the Shimla Agreement sought to stabilize the region.
- **The Watershed (1980s):** The Soviet-Afghan war provided a template and surplus weaponry. Infiltration surged followed by terror act, and innocent civilians (Kashmiri Pandits) were subjected to ethnic cleansing and forced to flee in a tragic demographic exodus.
- **The Islamist Shift (1990s-2000s):** The rise of Al-Qaeda and later ISIS has changed the character of the conflict. Secessionism was replaced by Islamist fundamentalism. Regional affiliates like **Lashkar-e-Toiba (LeT)** and **Jaish-e-Mohammed (JeM)** developed networks across 18 countries.

The Present Matrix (2026 Perspective)

The abrogation of Article 370 in 2019 was a structural reset. However, the threat remains "dynamic":

1. The Jammu Pivot and the Phalgham Trauma

The Valley is no longer the primary "bleeding point." Because the security grid in Srinagar and Baramulla is now impenetrable, terror groups have shifted focus to the rugged, forested terrain of the **Jammu region (Kathua, Reasi, Doda)**.

The **Phalgham terror attack** (referencing the brutal strikes on pilgrim convoys and army patrols) was a strategic shock. It proved that terrorists are moving away from populated towns into the "Southern Pir Panjal" hills. In the last two years, while terror incidents in the Valley dropped by nearly **70%**, the Jammu hills saw a sharp spike, with over **15 major encounters** in 2024-25 alone.

2. The "Faceless" Hybrid Threat

We are seeing the rise of the **Hybrid Terrorist**. These are not trained militants from across the border with long beards and fatigues. They are "part-timers"—young men with no prior criminal record who live normal lives by day and pick up a "sticky bomb" or a pistol by night. They target the most vulnerable: migrants, minorities, and local off-duty policemen. Because they have no "Digital Shadow" or police file, they are incredibly hard to track before they strike.

3. Operation Sindoor: The State's Digital Counter-Punch

In response to the Phalgham tragedy, the Indian state launched **Operation Sindoor**. This wasn't just a military operation; it was a "Technical Siege."

- **The Intelligence Shift:** Operation Sindoor used **Operation-Level Data Mining** to track the movement of "Over Ground Workers" (OGWs) who provide the logistics for hybrid cells.
- **The Result:** By deploying high-altitude drones and AI-powered thermal sensors in the Kathua-Reasi belt, the operation neutralized over **40 top commanders** and destroyed deep-forest hideouts that had been active since the 1990s. It has successfully broken the "command and control" of the new Jammu cells.

4. Tourism as the Ultimate Resilience

The best data point for 2026 is the sound of footsteps, not guns. Despite the terror at Phalgham, J&K saw a record **21.5 million tourists** in 2025. This "Economic Normalcy" is the state's greatest weapon. When a village in Pahalgam or a shop in Jammu earns from tourism, they lose the incentive to support the "merchants of chaos." The civilian "longing for peace" has finally become stronger than the insurgent's "threat of the gun."

II. The North East: The Mosaic of Ethno- sub nationalism

The North East is a theatre where the challenge is not "anti-India" sentiment in the classical sense, but rather a clash of competing tribal and ethnic aspirations.

1. The Cause: Periphery vs. Heartland

The region's conflict is rooted in a long history of tribal violence and the manifestation of **ethnic mobilisation**. Most states were formed through a violent evolutionary process (e.g., the reorganization of Assam). Illegal immigration remains the "mother of all grievances," altering demographics and fuelling local insecurities.

2. Evolution and Present Status

- **Institutional Innovation:** The Indian State responded not just with force, but with the **Sixth Schedule**, Autonomous Councils, and peace accords.
-
- **Present Status:** We are seeing the **"Act East"** transition. With the signing of several peace deals (ULFA, Naga & Bodo Accords) and the significant reduction of AFSPA (Armed Forces Special Powers Act) in several districts, the region is moving from a "conflict zone" to India's "gateway to ASEAN." But the there are the pockets of explosion as in Manipur.

1. Manipur crisis - the Ethnic Wound: Beyond Land and Identity

The crisis that exploded in May 2023 between the **Meitei** and **Kuki-Zo** communities has become a permanent scar. By early 2026, the state is physically divided by "Buffer Zones" manned by the Army. It is a "Civil War" in slow motion. The conflict isn't just about Scheduled Tribe (ST) status anymore; it is about **territorial sovereignty**. The state has effectively fractured into the "Valley" and the "Hills," with the civil administration struggling to bridge a gap made of blood and mistrust.

2. The Revelation: The Foreign "War Trainers"

The most sensational revelation of **March 2026** is the NIA's arrest of **six Ukrainian nationals** and an **American, Aaron Vandyke**, in the Northeast.

- **The Shock:** These weren't tourists. Investigations reveal they were "War Trainers" providing advanced tactical training to local insurgent groups.
- **The Drone Factor:** The use of sophisticated **attack drones** and IEDs in recent clashes—reminiscent of the battlefields in Eastern Europe—was not a coincidence. These foreign actors were reportedly teaching "Modern Guerilla Warfare" to both valley-based and hill-based militants.
- **The Geopolitical Trap:** For the first time, the "Western Hand" is being discussed not as a conspiracy, but as a charge sheet. It suggests that Manipur has become a laboratory for international "proxy warfare" on India's doorstep.

3. The Post-Crisis Matrix: A Hard Border

The "existing scenario" is one of extreme securitization. The Indian state has finally accepted that "soft borders" are a luxury we can no longer afford.

- **Suspension of FMR:** The **Free Movement Regime (FMR)** with Myanmar has been completely scrapped.
- **The "Iron Fence":** Construction of a 1,643 km fence along the Myanmar border is being fast-tracked. The government has realized that as long as the border is porous, the **"Golden Triangle"** drug money and foreign trainers will keep the fire burning.
- **Hybrid Insurgency:** We are seeing the rise of "Hybrid Insurgents"—locals who operate as civilians by day but use foreign-trained drone tactics by night.

Conclusion: The "Act East" at Crossroads

In 2026, the "Act East" policy—our grand vision for connectivity with SE Asia—is on life support. You cannot have trade routes through a war zone. The Manipur crisis is no longer an "internal grievance"; it is a national security emergency where local ethnic pain is being exploited by global actors. If we don't heal the wound in the Valley and the Hills, the Northeast may remain the "Achilles' Heel" of the Indian Republic.

III. Punjab: The Quelled Fire

The Punjab insurgency was perhaps the most dangerous threat to the secular fabric of India, involving a demand for a separate state based on religious identity.

The Cause and Resolution

- **The Secessionist Peak:** The 1980s saw the demand for "Khalistan" backed by cross-border support.
- **The Resolution Model:** Punjab serves as the "Gold Standard" for conflict resolution in India. It was settled through four parameters:

1. **Kinetic Action:** Targeted security operations to eliminate hardline terrorists.
2. **Sub-terranean Persuasion:** Dialogue with militants to bring them to the table.
3. **Political Integration:** Over-the-table discussions with those prepared to accept the Constitution.
4. **Cultural Sensitivity:** Respecting the religious and ethnic sentiments of the Sikh community.

Present Status

While the domestic situation is peaceful, the threat has moved **transnational**. The embers are now fanned by sections of the diaspora living abroad (UK, Canada, USA). In 2026, the challenge is not a ground insurgency in Ludhiana, but a **Digital/Information War** orchestrated from overseas.

The 2026 Outlook

As an aspirant, your analysis must reflect that India's counter-terrorism strategy has shifted from **"Management"** to **"Resolution."**

No	Theatre	Primary Driver	Strategy
1	**J&K**	Proxy War / Jihad	Multi-pronged: Security + PM's Reconstruction Plan + Unified Command.
2	**North East**	Ethno-Nationalism	Conflict Resolution: Autonomous Councils + Peace Accords + Act East.
3	**Punjab**	Transnational Secessionism	Vigilance: Countering diaspora-funded radicalization.

Conclusion

The "Inherited Insurgencies" are fading, but they are being replaced by **"Invisible Battlefields"** (Cyber and Hybrid warfare). The mission of the Indian State remains the same: to ensure that the development of the "last mile" outpaces the reach of the "last bullet."

Unit-6

The "Two-Front" war - (India – the theatre of Global Jihad)

The "Two-Front" challenge in internal security is defined as a **synchronized pincer movement** where the Indian state is forced to fight on two distinct yet overlapping battlefields:

1. **The physical Front:** The physical, state-sponsored proxy war orchestrated from across the border.
2. **The Psychological Front:** The invisible, digital radicalization of our own citizens—the "Gauz – wa- hind." & Global Jihad.

It is the lethal synchronisation of a hostile neighbour's military doctrine with a global, borderless ideology.

The Typical Nature: War without Uniforms

The nature of this war is **Asymmetric and Hybrid**. It does not seek to capture land; it seeks to capture the **National Narrative** and **Communal Harmony**.

- It is **Non-Linear:** An attack in a remote valley in Kashmir is timed to trigger a riot in a metropolis like Bengaluru.
- It is **Grey Zone:** It operates just below the threshold of open conventional war, making a decisive military response difficult without risking a nuclear escalation.

The Internal Security Challenge: Subversion from Within

Why is this an internal security nightmare? Because it turns the **Strengths of a Democracy** into its **Vulnerabilities**.

- **Our Diversity:** Used as a fault line to create "The other."
- **Our Freedoms:** The internet and free speech are weaponized to spread venomous propaganda.
- **Our Justice System:** Radicalized actors exploit the slow pace of Indian courts to build a narrative of "victimhood."

It is a challenge because the "enemy" is no longer just a soldier in a green uniform; it could be a radicalized youth in a suburban cyber-cafe who has never picked up a gun but can paralyze a city through a coordinated social media "flash-protest."

Universality vs. India's Distinctiveness

While the world faces the scourge of radicalization, India's "Two-Front" wound has a unique, more jagged edge.

- **The Universal Factor:** Much like France or the UK, India faces the "Global Wahabi - Salafi Jihad"—a borderless ideology that seeks to replace the nation-state with a global caliphate.
- **The Indian Exception:** Unlike the West, India has a **State Sponsor** (Pakistan) that has institutionalized this ideology as a low-cost tool of foreign policy. We are not just fighting "ideas"; we are fighting a neighbor's **Inter-Services Intelligence (ISI)** which provides the logistics, the funding, and the escape routes. This "Neighborhood Effect" makes our challenge permanent and existential.

How it Wounds India: The Two Types of Trauma

This pincer movement inflicts two specific types of wounds on the Indian psyche:

1. The Proxy War (The Physical Wound)

This is the "Old" Front—the brutal reality of **Lashkar-e-Taiba (LeT)** and **Jaish-e-Mohammed (JeM)**.

- **The Wound:** It targets our **People Confidence on State**. By striking symbols of our growth (Parliament, Taj Hotel, financial hubs), it seeks to tell the world that India is an "unsafe destination." It keeps the Indian Army bogged down in "Counter-Insurgency" roles, bleeding our defense budget and distracting us from our global ambitions.

2. The Digital Caliphate (The Home grown Wound)

This is the "New" Front—the shift from the organized cells of the SIMI era to the **"Lone Wolf"** and **ISIS-inspired** actors.

- **The Wound:** It targets our **Social Cohesion**. Radicalization is now "Open Source." A youth in Kerala or Maharashtra is recruited via Telegram or encrypted "Dark Web" forums.
- **The Impact:** These homegrown actors don't need a supply chain from Lahore; they use locally available tools—a car, a knife, or a basic IED. The wound here is deep-seated suspicion between communities, which is exactly what the "Two-Front" strategy desires: an India at war with itself.

"Two-Front War" is a form of terrorism

The concept of a **“Two-Front War” in terrorism** refers to the simultaneous threat India faces from:

1. **Proxy war - State-sponsored cross-border terrorism**.
2. **Homegrown radicalization enabled by digital platforms**

The first involves external groups like LeT/JeM aiming to "bleed" the nation physically. The second targets our internal fabric via **"Lone Wolf"** actors radicalized entirely online. This hybrid strategy synchronizes physical strikes with psychological subversion, targeting India’s economic stability and communal harmony, requiring both military vigilance and robust, community-led counter-radicalization frameworks.

This dual challenge makes terrorism more **complex, decentralized, and persistent**.

1. The Proxy War (The Physical Wound)

The Definition: Kinetic Diplomacy

The Proxy War is the use of non-state actors by a state to achieve strategic military and political goals without engaging in a full-scale, conventional war. It is "kinetic" because it involves physical violence—bullets, IEDs, and infiltration—but it is "proxy" because the hands on the trigger belong to "mujahideen" while the eyes behind the scope belong to Rawalpindi (ISI) .

The Reasons:

1. The Primary Reason: The Existential Crisis

The fundamental driver is **Pakistan’s existential insecurity**. Since 1947, and more acutely since 1971, the Pakistani "Deep State" has viewed a stable, secular, and economically rising India as a threat to its own relevance. The "Kashmir Issue" is merely the convenient mask for a deeper pathological need to prevent India from achieving its global potential.

2. The Inducement Reason: The 'Holy' Motivation

If the primary reason is strategic, the inducement is **ideological**. The foot soldiers are recruited using the toxic Islamic myth of **"Ghazwa-e-Hind"** and the narrative of creating dar – ul – Islam (Islamic India). This religious fervor is the fuel that allows a handler in

Muridke & other terror schools to convince a youth to cross a freezing mountain pass with a suicide vest.

The Role of Pakistan (The Puppeteer)

In India, we often make the mistake of distinguishing between the Pakistani civilian government and it's military. For the 2026 security matrix, this is a dangerous delusion.

- **The ISI-Terror Nexus:** The Inter-Services Intelligence (ISI) acts as the CEO of this proxy industry. It provides the **"Launch Pads"** along the Line of Control (LoC), the high-grade communication equipment, and the "Ratlines" for infiltration.
- **State Policy:** Terrorism is Pakistan's primary export. It uses these proxies to keep the Indian Army permanently deployed in a counter-insurgency role, draining our exchequer and slowing our move toward a leaner, "tech-first" military.

The Actors: Important Terror Groups

No	Group	Ideology/Focus	Key Operating Style
1	**Lashkar-e-Taiba (LeT)**	Salafism / Pan-Islamic	High-visibility "Fidayeen" attacks (e.g., Mumbai 26/11).
2	**Jaish-e-Mohammed (JeM)**	Deobandi / Kashmir focus	Heavy use of IEDs and suicide car bombs (e.g., Pulwama).
3	**The Resistance Front (TRF)**	Secular "Facade"	A "rebranded" LeT/JeM to escape FATF scrutiny; targets soft targets/civilians.
4	**Hizbul Mujahideen (HM)**	Indigenous / Ethnic	Historically the "local face" of the insurgency, now largely sidelined by JeM/LeT.

The Recent Flashpoints (2024–2025)

As we approach 2026, the theatre of the proxy war has mutated to expose the fragility of "normalcy."

1. **The Jammu Pivot (Late 2024):** Audacious ambushes in **Kathua** and **Reasi** shifted the kinetic front to Jammu's difficult hills, forcing a tactical overstretch of security forces.
2. **The Pahalgam Menace (2024–25):** Strategic strikes on tourists and locals in the **Lidder Valley** hit the economy where it hurts most, proving that no "safe zone" is truly secure.
3. **2025 Targeted Killings:** The use of **"Hybrid Terrorists"**—radicalized civilians with clean records—to execute migrants and minorities. This is a cold attempt to force a demographic retreat and dismantle the state's claims of a peaceful post-Abrogation era.

The Nature of the Menace: A Permanent State of Siege

The Proxy War is not a "problem" to be solved; it is a **"condition" to be managed**. Its nature is:

1. **Asymmetric:** A few thousand rupees and a radicalized mind can force a multi-billion dollar response from the Indian state.
2. **Deny-able:** Pakistan maintains a "Plausible Deniability" that allows it to engage in trade and diplomacy while simultaneously fuelling bloodshed.
3. **Cyclical:** It ebbs when India's counter-insurgency is tight and flows the moment there is a political or administrative lapse.

2. The Digital Caliphate (The Home grown Wound)

The Primary Reason: The Void of Identity

The fundamental reason for the rise of the Digital Caliphate is a **Crisis of Belonging**. For decades, our secular state has failed to provide a national narrative strong enough to tether the restless youth to the idea of India. When the state is seen only as a slow, corrupt provider of licenses and a clumsy arbiter of disputes, the globalized youth looks elsewhere.

In the vacuum left by a lack of genuine civic education and a sense of shared destiny, the transnational "Ummah" narrative—repackaged with high-definition production values—offers a sense of purpose. It is not always poverty that drives this; often, it is a well-educated, tech-savvy individual seeking a "heroic" identity in a world they perceive as hostile.

The Inducement Reason: The Alchemic Power of the Algorithm

If the reason is identity, the inducement is **Digital Alchemy**.

- **The E-Madrasa:** Radicalization has moved from the physical ghetto to the encrypted one. The recruiter isn't a bearded man in a basement; it's a bot or a distant handler on Telegram or Signal.
- **The Victimhood Narrative:** Every global event—from a skirmish in Gaza to a legislative change in India—is live-streamed, edited with stirring music, and fed to the vulnerable through an algorithm designed to confirm their worst fears. It induces a "Pre-Traumatic Stress Disorder," where the youth is convinced they are under attack and that violence is the only "defensive" response.

The Actors: From Organized Cells to the 'Lone Wolf'

The 2026 landscape has seen a shift from the structured hierarchies of the past to a "franchise" model of terror.

- **ISIS-K (Khorasan Province):** While the physical caliphate fell in the Levant, the Khorasan module remains the primary ideological exporter to India.
- **AQIS (Al-Qaeda in the Indian Subcontinent):** Reinvigorated by the geopolitical shifts in our neighborhood, focusing on local recruitment for global goals.
- **The 'Banned' Shadows:** After the ban on the PFI, we have seen the emergence of "Clandestine Modules"—small, disconnected groups that operate without a central command, making them nearly impossible for the IB to map.
- **The Lone Wolf:** The ultimate actor—an individual with no prior record, radicalized entirely online, who strikes with a kitchen knife or a rented truck.

Recent terror events (2024–2025)

As we look back from the vantage point of 2026, two types of events define this menace:

1. **The 'Deepfake' Riots (Early 2025):** A milestone in hybrid warfare where AI-generated videos of a religious site being desecrated were circulated in the hinterland. The resulting communal frenzy was not "organic"; it was a "Digital Jihad" designed to shatter the narrative of a stable, rising India.

2. **The Multi-City 'Sleeper' Busts (Late 2024):** The NIA's coordinated raids in Maharashtra and Karnataka revealed that the "Home grown Wound" had moved into the IT sector, with tech professionals building encrypted communication platforms for global jihadist entities.

The Nature of the Menace: An Open-Source Insurgency

The Digital Caliphate is a menace that is **Fluid, Invisible, and Open-Source**.

- **It is 'Leaderless':** There is no "head" to cut off. If you ban one platform, they migrate to another. If you catch one handler, ten others emerge from the dark web.
- **It Weaponizes Development:** It uses the same high-speed internet and Digital Public Infrastructure (DPI) that India uses for growth.
- **The Internal Fault Line:** Its primary goal is to trigger a state crackdown that is so heavy-handed it alienates the moderate majority. It wants the state to be seen as the "oppressor," thereby creating a fresh crop of recruits.

Insight for the Aspirant:

In your Mains answer, argue that the "Digital Caliphate" cannot be defeated by the UAPA alone. It requires **"Cognitive Sovereignty."** We need a counter-narrative that is as digitally slick and emotionally resonant as the extremist one. The war is for the "hearts and minds" of the youth, and as of now, the algorithm is often in the hands of the enemy.

The Government of India's measures on the two Fronts War.

1. Policy Measures: From Dossiers to Destruction

The current policy is defined by **Zero Tolerance**. The state has finally realized that you cannot negotiate with an ideology that denies your right to exist.

- **The 'Sindoor Doctrine' (2025-26):** Emerging from the 2025 conflict, this policy dictates that India will no longer differentiate between the terrorist and the state that hosts him.
- **Economic & Diplomatic Attrition:** The decision to hold the **Indus Waters Treaty** in abeyance ("Blood and water cannot flow together") and the total suspension of trade and cultural ties signify a shift from purely military to "Whole-of-Government" retaliation.
- **PRAHAAR Policy (2026):** A comprehensive national strategy focusing on **Prevention, Response, Aggregation of Capacities, Human Rights, and Attenuating Conditions.**

2. Institutional Measures: The Iron Grid

We have stopped fighting a 21st-century war with a 19th-century bureaucracy.

- **NIA (National Investigation Agency):** NIA professionalism, now enable the "Gold Standard" with a **95% conviction rate**, focusing on dismantling the financial ecosystems of terror.
- **NATGRID & MAC:** The seamless integration of 11 central agencies and state police ensures that intelligence is "actionable" and shared in real-time, ending the era of departmental silos.
- **CIBMS (Comprehensive Integrated Border Management System):** The "Smart Fence"—a technological wall of sensors, thermal imagers, and AI-driven surveillance that makes the physical border nearly impermeable.

3. Counterterror Operations: The New Normal

1. The Precedents: Surgical Strikes (2016 & 2019)

The 2016 Uri response and the 2019 Balakot air strikes shattered the myth of Pakistan's "nuclear blackmail." They established that India would strike the source of the wound, regardless of the map.

2. The Watershed: Operation Sindoor (May 2025)

This was India's most expansive and technically sophisticated response since 1971.

- **The Trigger:** The barbaric **Pahalgam attack** (April 22, 2025), which targeted 26 innocent tourists.
- **The Strike:** Launched on May 7, 2025, the tri-services operation targeted **9 terror launchpads** simultaneously using precision-guided missiles and loitering munitions.
- **The Result:** Over 100 terrorists neutralized without targeting a single Pakistani military installation, demonstrating a clinical "Strategic Restraint" paired with "Disproportionate Retaliation."

4. Addressing the Home grown Wound

Radicalization is the "Internal Front." The government's approach has moved beyond just police action to **Cognitive Sovereignty**.

a) **The PFI Ban legacy:** Dismantling organized radicalization pipelines.
b) **Hybrid Terrorist Monitoring:** Using Big Data and AI to track individuals with "clean records" who are being radicalized in the shadows of the dark web.
c) **Counter-Narratives:** Engaging community leaders and using digital platforms to puncture the extremist's "victimhood" narrative with the reality of India's inclusive growth.

The road to 2047 requires an India that is **un-blackmailable**.

Suggestions :

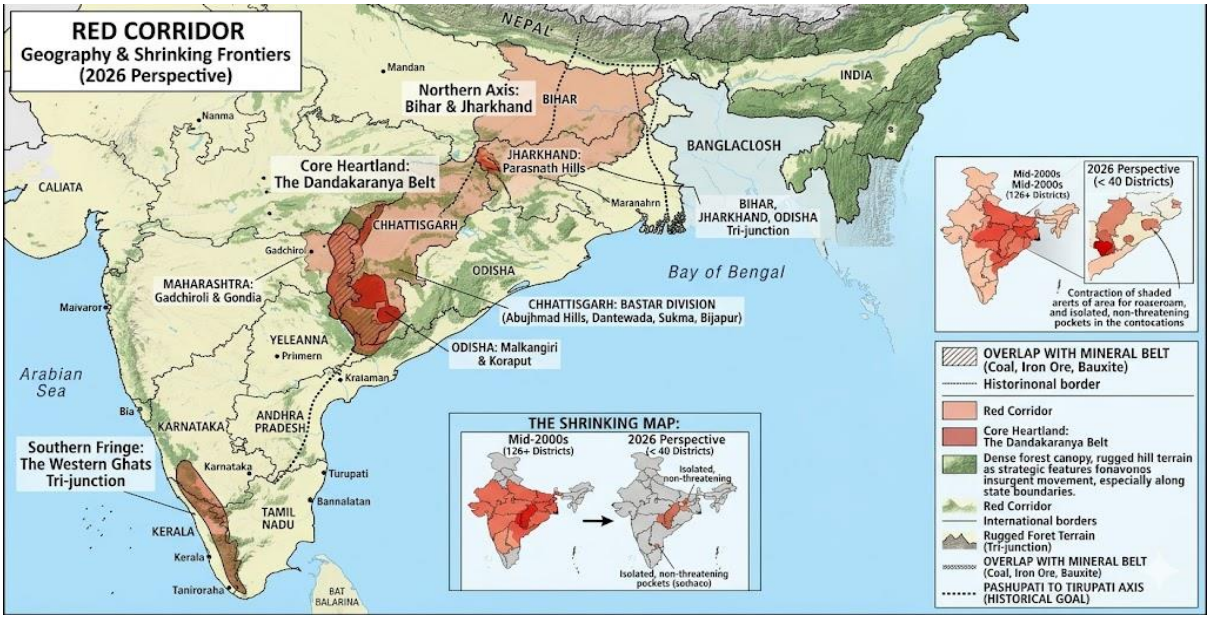
1. **Cyber-Sovereignty:** We must develop our own encrypted communication protocols to deny the "Digital Caliphate" its playground.
2. **Police Modernization:** The "Last Mile" of security is the local police station; it must be as tech-savvy as the NIA.
3. **Strategic Resilience:** Maintaining the "Whole-of-Government" pressure on state sponsors until the cost of supporting terror exceeds the benefit.

Conclusion:

In 2026, India is no longer a "soft state" issuing protests. It is a Republic that has acknowledged that internal security is indispensable for economic prosperity. The message of **Operation Sindoor** and the **PRAHAAR Policy** is clear: the Indian State is no longer interested in managing and reacting to the menace but it is committed to its total **Elimination**.

Unit -7

Left-Wing Extremism in India



The Genesis of the Naxalbari Moment

The pathology of Left-Wing Extremism (LWE) in India did not emerge from a vacuum; it was a violent rejection of the post-colonial democratic settlement. On **March 3, 1967**, in the Siliguri sub-division of West Bengal, a breakaway faction of the CPM ignited what they termed an "agrarian revolution."

Named after the village of **Naxalbari**, the movement was led by ideologues like **Charu Majumdar** and **Kanu Sanyal**, who were convinced that the Indian "objective condition" was ripe for a Maoist-style peasant uprising.

They sought to rectify land inequities—often genuine grievances regarding the failure of the **West Bengal Estate Acquisition Act of 1953**—through the "annihilation of class enemies." However, as history often dictates, the romanticism of the revolution quickly degenerated into a fratricidal menace, particularly when the leadership chose to support Pakistan during the 1971 Bangladesh Liberation War, leading to an ideological crisis and the eventual arrest of Majumdar in 1972.

Evolution: From Splintered Groups to a Militarized dalams

The movement has traversed a jagged path over five decades:

1. **The Hibernation (1970s):** Following state crackdowns, the movement fragmented into localized splinter groups.
2. **The Resurgence (1980s-1990s):** Two dominant poles emerged: the **People's War Group (PWG) dalams** in Andhra Pradesh and the **Maoist Communist Centre (MCC)** in Bihar. The PWG successfully tapped the tribal grievances in the **Dandakaranya** belt, while the MCC's in Bihar morphed the brutal caste warfare against landlord "Senas" like the **Ranvir Sena**.

   Operational Highlights: The Jehanabad Jailbreak (2005): A spectacular failure of state capacity where 1,000 Maoists stormed a jail to free their leader, Ajay Kanu.

3. **The Consolidation (2004-Present):** On **September 21, 2004**, the merger of PWG and MCC into the **CPI (Maoist)** signalled a new epoch of militarization. The shift went from agrarian protest to high-intensity insurgency, utilizing sophisticated weapons (AK series) and a terrifying expertise in IEDs.

The Geography of the Red Corridor

The LWE geography is fundamentally tied to India's **tribal heartland and forest tracts**. Known as the "Red Corridor," it historically spanned from the Pashupati (Nepal) to Tirupati (Andhra Pradesh).

- **The Dandakaranya Belt:** This remains the hub of LWE—a dense forest tract covering parts of **Chhattisgarh (Bastar)**, Odisha, Maharashtra, and Andhra Pradesh.
- **The Terrain as an Ally:** The rugged topography provides the Maoists with "liberated zones" where the writ of the Indian state has historically not exist, allowing for the establishment of parallel administrations known as **Janatana Sarkars** or **Praja Courts**.

The Root Causes: Governance Vacuums and Identity

LWE thrives where the state is absent or perceived as predatory.

- **Land Alienation:** The persistent failure to implement land reforms and the dispossession of tribal lands for mining and industrial projects.

- **The Governance Deficit:** As the ARC notes, "Praja Courts" meted out "swift justice" only because the formal legal system was seen as an instrument of the elite.
- **Tribal Exploitation:** The marginalization of the forest-dwellers created a vacuum that the Maoists filled, positioning themselves as "saviors" against an exploitative administration.

Implications: A Challenge to the Idea of India

LWE is not merely a law-and-order problem; it is an existential challenge to the Republic's sovereignty.

- **Economic Stalling:** By targeting infrastructure—railways, telecommunications, and schools—the Maoists ensure the "perpetual backwardness" that fuels their recruitment.
- **Democratic Erosion:** The targeting of political functionaries (as seen in the brutal hits on CPM leaders in West Bengal or the 2013 Darbha Valley attack) seeks to hollow out the democratic space.

Government Measures and Counter-Operations

The state's response has evolved from the "sledge-hammer" approach to a more nuanced **Security-Development Nexus**.

1. **The Greyhounds Model:** Andhra Pradesh's elite unit proved that specialized training, paired with local intelligence, could dismantle Maoist bases (e.g., the Nallamala forest victory).
2. **Institutional Framework:** The **Unified Command** mechanism and the **SAMADHAN** doctrine (Smart Leadership, Actionable Intelligence, etc.).
3. **Salwa Judum:** A controversial tribal resistance movement in Chhattisgarh that, while effective in some pockets, raised deep ethical and human rights concerns regarding the militarization of civilians.
   - **Operation Green Hunt:** The broad name for the paramilitary offensive launched in the late 2000s.

The 2026 Perspective: The Final Push

As of **2026**, the Union Home Ministry has set a definitive target for the **total elimination** of LWE.

The Indian state has finally stopped playing a game of "hide and seek" in the jungles. The current strategy is a clinical **Security-Development Nexus** that treats the insurgency like a wound that needs both cleaning and healing. By 2026, the "Red Corridor" has been squeezed from 126 districts to a mere handful of core pockets.

In the once-impenetrable **Abujhmad** forests, the "Sarkar" isn't just sending boots on the ground; it is using high-tech drones and satellite imagery to flush out the last cadres. **Fortified police stations** now act as permanent anchors of sovereignty, ensuring that once a territory is cleared, the Maoists can never return to claim it.

However, the state knows that security can only "clear" the land; only development can "hold" it. The focus has shifted entirely to the **"last mile" of connectivity**. Through massive schemes like **PM-JANMAN** and the **Aspirational Districts Programme**, the government is saturating these regions with 4G towers, metalled roads, and bank branches.

The idea is to make the state visible and useful. When a tribal youth gets a bank account or a bridge reaches a remote village, the Maoist narrative of an "oppressive state" falls apart. In 2026, the bridge has become as lethal to the insurgency as the bullet.

For those still carrying guns, the state has built a "golden bridge" to return to society. The 2026 **Surrender and Rehabilitation Policy** is designed to hollow out the Maoist ranks from within. It offers immediate financial assistance, life insurance, and vocational training to any cadre who chooses the ballot over the bullet.

By treating the foot soldier as a victim of a dying ideology rather than just a criminal, the state is winning the human war. It is much harder for a Maoist commander to keep his group together when his soldiers know they can have a dignified life and a real job by simply walking into a police station.

As we approached the **March 2026 deadline** for a "Naxal-free India," the final phase of the battle has moved to the cities and the digital world. While the physical "Red Corridor" is almost gone, the "Urban Naxal" networks—the intellectual and logistical support in our cities—remain a high-priority concern.

These "remnant cells" use the internet and the legal system to keep the movement alive in the shadows. The 2026 outlook is one of cautious victory; the forests are being reclaimed, but the state must now win the "War of Narratives" to ensure this home-grown wound never reopens.

To Sumup.

The bullet can kill a Naxalite, but only a road/school can kill Naxalism. The ARC's lesson remains timeless—the state must use the "fly-swatter" of targeted operations and the "healing touch" of development, rather than the "sledge-hammer" of indiscriminate force.

Unit -8

Naxalism

The Definition: A War against the Republic

Naxalism is not just a "crime problem." It is an armed insurgency led by Maoists who want to overthrow Indian democracy. They do not believe in the Election process; they believe in the "Protracted People's War." Their goal is to capture power through the barrel of a gun, using the poor as their foot soldiers.

The Origin: The Naxalbari Spark (1967)

It began in a small, dusty village called **Naxalbari** in West Bengal. What started as a local fight between a tribal peasant and a landlord was called "Spring Thunder" by China. Led by **Charu Majumdar** and **Kanu Sanyal**, it was a violent rejection of the Indian state. It told the peasant that the only way to get justice was to "annihilate" the class enemy.

The Causes:

The "Sarkar" (Government) effectively handed the matchbox to the Maoists through decades of neglect and broken promises.

1. **Land Reform Failure:** The law books in Delhi said land should belong to the tiller. But on the ground, the "Lutyens' elite" and local strongmen ensured the

papers never moved. The poor remained landless, and the Maoists promised them a piece of the earth.

2. **Unpopular Forest Policies:** For centuries, tribes (Adivasis) lived in the forests. Suddenly, the state made them "encroachers" on their own ancestral land. This insult was the best recruitment tool the Naxalites ever had.
3. **Development Deprivation:** In the heart of India, there were places with no roads, no electricity, and no schools. When the state is invisible, the man with the AK-47 becomes the provider.
4. **Food Security & Jobs:** If a tribal youth has an empty belly and no job, the "party" provides a uniform, a weapon, and a sense of purpose. Hunger is the greatest recruiter for a revolution.
5. **Governance Deficit:** The local administration was often corrupt or simply didn't exist. This "vacuum" allowed Naxalites to set up **"Janatana Sarkars"** (parallel governments) and **"Kangaroo Courts"** to deliver instant, brutal justice.

Evolution of Naxalism

The movement has moved through four distinct phases:

1. **Phase I (1967–1975):** The early, chaotic years. It was violent and led by students and peasants. It was eventually crushed during the Emergency.
2. **Phase II (1980s–2004):** The movement went into the deep jungles. Two major groups grew powerful: the **People's War Group (PWG)** in Andhra Pradesh and the **Maoist Communist Centre (MCC)** in Bihar.
3. **Phase III (2004–2014):** The "Red Corridor" phase. The PWG and MCC merged to form the **CPI (Maoist)**. Suddenly, a "Red Corridor" stretched from the Nepal border to Andhra Pradesh. Former PM Manmohan Singh called it India's "greatest internal security threat."
4. **Phase IV (2014–2026):** The Shrinking Frontier. The state finally woke up. Through better security and massive spending on roads and bridges, the "Red Corridor" has been broken into small, isolated pockets.

As the **March 2026 deadline** for a "Naxal-free India approached," the lesson is clear. Naxalism survived in the shadows cast by the state's neglect. It was a "Homegrown Wound." Today, as the road reaches the village and the tribal child reaches the school, the Maoist ideologue loses his followers. The victory of 2026 is not just a military one; it is the victory of the Indian Republic finally showing up for its forgotten citizens.

The Dark Nexus: Naxal-Narco-Terror Linkage

In the early days, Naxalism was about land. In 2026, it is about **Money and Power**.

- **The Narco-Connection:** The Maoists have moved from "protection money" to active participation in the drug trade. They facilitate the movement of narcotics from the **Golden Crescent** into the heartland to fund their arsenal.
- **The Terror Tie-up:** Agencies have found clear links between the CPI (Maoist) and external state actors like the **ISI**. There is a "barter system" where drugs and fake currency are exchanged for sophisticated weapons like AK-series rifles and sniper gear.
- **The Organized Crime Model:** The Maoists now operate like a corporate mafia, taxing mining companies and contractors. This money doesn't go to tribal welfare; it goes to the "War Chest."

The Present Face of Naxalism: Three Fronts

Naxalism in 2026 is not a single monolith. It operates on three distinct levels:

1. **The Guerrilla Front:** The armed "Dalams" in the deep forests of **Bastar and Abujhmad**. They use IEDs and ambushes to keep the state out.
2. **The Urban Front:** Often called **"Urban Naxals,"** these are the ideologues in cities. They provide the "legal shield" and "international propaganda" that protects the forest fighters.
3. **The Hybrid Front:** Individuals with "clean records" who live in villages but act as eyes and ears for the insurgents. They are the most difficult to track.

The Organizations:

1. **CPI (Maoist):** The "parent" company. Formed in 2004, it remains the most lethal entity.
2. **PLFI (People's Liberation Front of India):** A breakaway group in Jharkhand that is essentially a high-end extortion gang.
3. **TPC (Tritiya Prastuti Committee):** Another faction that often clashes with the CPI (Maoist) over the "spoils" of the mining belt.

Government Measures: From 1967 to 2026

The Indian state's response has moved from "blind force" to "smart governance."

- **The Early Years (1970s):** Operation Steeplechase was a pure military "sledgehammer" approach. It crushed the first wave but didn't heal the wound.
- **The Institutional Phase (2000s):** The creation of the **Unified Command** and the **Greyhounds** in Andhra Pradesh showed that specialized local police are better than general central forces.
- **The SAMADHAN Doctrine (2017–2026):** The current "Holy Grail" of counter-insurgency. It focuses on **S**mart Leadership, **A**ctionable Intelligence, and **H**arnessing Technology like drones and satellites.

Recent Countermeasures & the 2026 Deadline

The Union Government has set **March 31, 2026**, as the final deadline for a "Naxal-free India."

- **Operation Prahaar:** A sustained, multi-state offensive to flush out the top leadership from their last hideouts.
- **Fortified Police Stations:** Over 600 police stations have been turned into "mini-fortresses" to ensure the state's presence is permanent.
- **PM-JANMAN & RRP:** Massively funding roads and 4G towers in tribal areas to bridge the "Development Deficit."

The "Red Corridor" is shrinking because the state is finally "showing up."

The Way Forward:

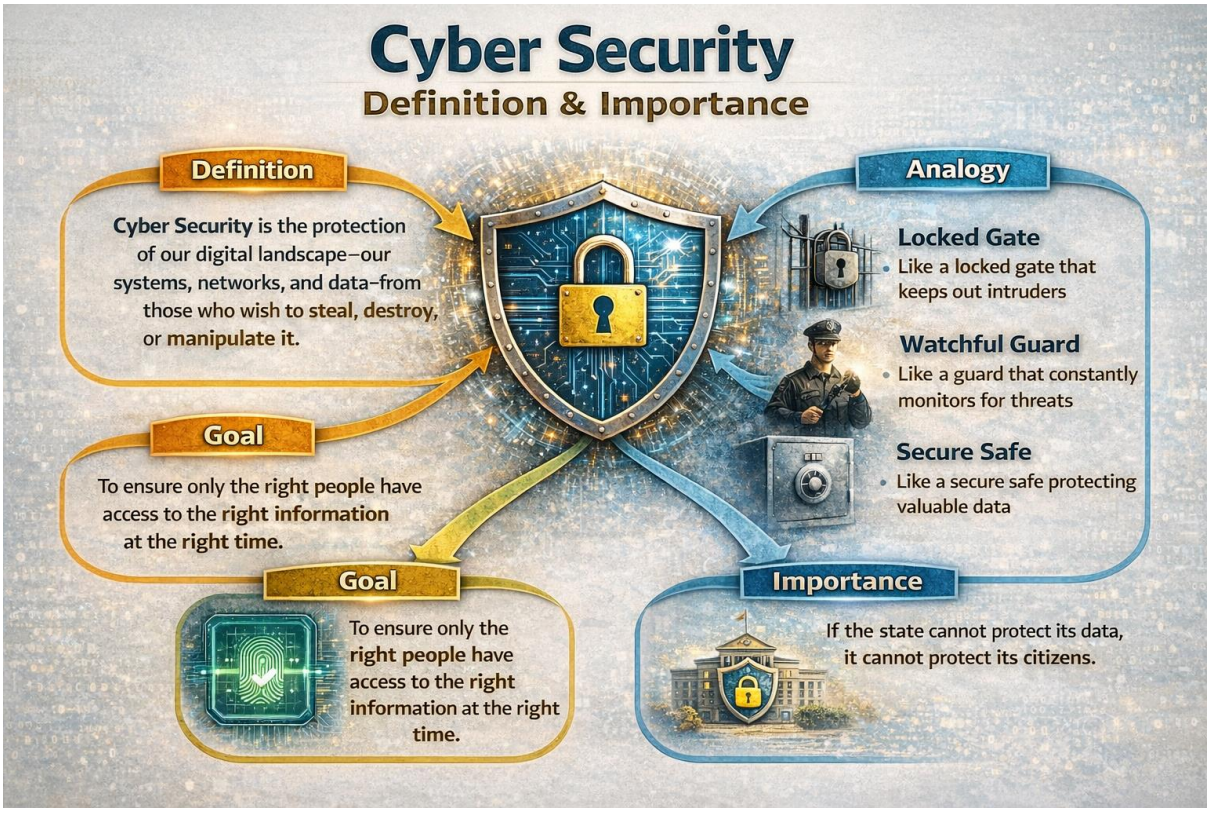
1. **Digital Sovereignty:** We must monitor the dark web where "Urban Naxals" and "Narco-merchants" coordinate.
2. **Psychological War:** We need better stories. The state must prove that the "Ballot" brings more food than the "Bullet."
3. **Zero-Vacuum Governance:** The moment a forest is cleared of Naxals, a school and a bank must open the next day.

Conclusion:

By 2026, Naxalism is a dying flame. It survived on the state's neglect, but it is being extinguished by the state's resolve. The victory is not when the last Naxal is caught, but when the last tribal child in Bastar feels that the Indian Tricolour is their own.

Unit -9

Cyber Security



The Definition:

Cyber Security is the protection of our digital landscape—our systems, networks, and data—from those who wish to steal, destroy, or manipulate it.

In simple terms, it is the digital equivalent of a locked gate, a watchful guard, and a secure safe. It is the art of ensuring that only the right people have access to the right to information at the right time. If the state cannot protect its data, it cannot protect its citizens.

Elements of Cyber Security: the Armoury:

To defend a nation, you don't just guard the palace; you guard the roads, the messengers, and the archives.

1. **Network Security:** This is the **Digital BSF**. It protects the networks from intruders using firewalls and encryption to ensure that the traffic flowing through our servers is legitimate.
2. **Application Security:** Think of this as the locks on your software. It ensures that apps (like UPI or Digi Locker) don't have "backdoors" that hackers can use to sneak in.
3. **Endpoint Security:** This protects the devices in your hand—your phone, your laptop, your tablet. In 2026, every smartphone is a potential entry point for an enemy.
4. **Data Security:** Protecting the **"New Oil."** It uses encryption to turn our secrets into unreadable code, so even if a thief steals the file, they cannot read the contents.
5. **Cloud Security:** As we move our data to the "Cloud" (remote servers), we must ensure these digital warehouses are not misconfigured or left open to global predators.
6. **Mobile Security:** This targets the "spy in your pocket." With the rise of 5G and 6G, mobile-specific Trojans and spyware are the new frontline.
7. **Disaster Recovery & BCP:** What happens when the screen goes black? This is the "Plan B." It ensures that even after a massive attack, the power grid, banks, and hospitals can reboot and continue working.
8. **End-User Education:** The **Weakest Link**. You can have the best firewall in the world, but if a clerk clicks on a "phishing" link, the gates fly open. Education is the digital vaccine.

The Significance:

1. The 2013 Wake-up Call

Before 2013, India treated cyber security as a low-priority IT issue. Then came the **Snowden Revelations**. We realized that global powers were spying on our leaders and citizens with absolute impunity. This led to India's first **National Cyber Security Policy (2013)**. It was the moment we realized that digital dependence without digital defense is a trap.

2. The 2025-2026 Reality: The AI Era

The threat has mutated. According to the **India Cyber Threat Report 2026**, our nation faced over **265 million attacks** in the last year alone.

1. **AI-Driven Attacks:** Hackers now use Artificial Intelligence to create "Deepfakes" and automated phishing emails that look perfectly legitimate.

2. **Targeting Critical Infrastructure:** We are no longer just seeing data theft. We are seeing attempts to shut down our power grids, sabotage our airports, and paralyze our hospitals (like the AIIMS attack).
3. **Geopolitics:** Cyber attacks are now the "first strike" in modern conflicts. Before a tank moves, the internet goes down.

In 2026, every Indian with a smartphone is a soldier on the digital front. The government is doing its bit with the **SAMADHAN** doctrine and **CERT-In** alerts, but the real victory lies in **"Digital Hygiene."** We must stop being "rule-takers" in global tech and become "rule-makers." True sovereignty in the 21st century is not just about defending our borders of soil; it is about defending our borders of bits and bytes. If we fail here, we fail everywhere.

Defining the Cyber Menace- The Vocabulary & Example

To fight a war, you must first name the enemy. In 2026, the threats come in four distinct flavors:

1. **Cyber Threat:** This is the "dark cloud." It is any possible danger that might exploit a vulnerability to breach security and cause harm.
   - *Example:* A simple "phishing" email sent to a government clerk to steal their password.
2. **Cyber Crime:** This is about **Greed**. It is the use of computers to commit traditional crimes like theft, fraud, and defamation.
   - *Example:* The "Jamtara" model of digital looting or "Ransomware" where hackers lock your files and demand money to release them.
3. **Cyber Warfare:** This is about **Power**. It is a state-sponsored attack on another nation's digital infrastructure.
   - *Example:* Chinese state-backed groups planting malware in India's regional power grids to cause a blackout during a border standoff.
4. **Cyber Terror:** This is about **Fear**. It is the use of cyber attacks by non-state actors (like ISIS or LeT) to create panic, spread radicalization, or damage the economy.
   - *Example:* Hacking into a national news channel's feed to broadcast a fake, terrifying message during a festival.

The Shield: Elements of Cyber security

The state protects the digital heartland through several layers:

- **Network & Application Security:** Checking the "roads" and the "software" for holes.

- **Data Security:** Locking the "safe" with high-grade encryption.
- **Cloud & Mobile Security:** Protecting the data that sits on remote servers or in your pocket.
- **The Human Factor:** Educating the end-user. In 2026, the biggest vulnerability is not a weak firewall; it is a careless click.

The Crucial Fronts of Cyber security: Where India is Vulnerable

In 2026, a single line of code can do more damage than a thousand tanks. We must protect our "Critical Information Infrastructure" (CII).

1. Defense & Sensitive Documents

The days of stealing paper files are over. Today, foreign spies seek the "Digital Blueprints" of our Tejas jets and nuclear submarines. If our **Sensitive Documents** are leaked, our military edge disappears instantly. Our Defense networks must be "Air-Gapped" (disconnected from the public internet) to stay safe.

2. Communication Networks

This is the "Nervous System" of the Republic. If an enemy shuts down our 5G/6G networks, the government cannot talk to its people, and the army cannot talk to its commanders. It would be a "Digital Blindness" that leads to total chaos.

3. Kinetic Targets: ATC & Railway Management

This is where cyber attacks become **deadly**.

- **Air Traffic Control (ATC):** If a hacker takes control of ATC management, they can cause mid-air collisions without firing a shot.
- **Railway Traffic:** By manipulating the "Signaling System," an enemy can cause massive train accidents, paralyzing the nation’s lifeline and causing thousands of deaths.

4. Science & Tech Research Centres & Premier Institutions

Our IITs, ISRO, and DRDO are the "Brains" of India. In 2026, we face **"Digital Colonialism"** where adversaries try to steal our Research & Technology (IP Theft) to jumpstart their own industries. Protecting these premier institutions is about protecting India's future economic growth.

The Concerns: A Nation under Digital Siege

In 2026, the threat is no longer just a bored teenager hacking a website. It is about **Survival**.

- **AI-Powered Malice:** The most terrifying concern today is the use of Artificial Intelligence. Hackers now use "Deepfakes" to impersonate officials and "Automated Malware" that learns to bypass our defenses in real-time.
- **State-Sponsored Sabotage:** We are seeing "Digital First Strikes" by adversaries. They target our power grids, water systems, and banking networks to paralyze the nation without firing a single bullet.
- **The Ransomware Pandemic:** Our hospitals, small businesses, and even government departments are being held to ransom. Criminals lock our data and demand millions in cryptocurrency.
- **Identity Theft:** With the "Digital Caliphate" and organized gangs, your Aadhaar, bank details, and personal photos are being harvested on the **Dark Web** to fuel fraud and radicalization.

The Challenges of Cyber security:

Fighting a digital war is harder than fighting a physical one for three simple reasons:

1. **The Invisible Enemy:** How do you strike back when you don't know where the attack came from? Hackers use "proxies" and "mule accounts" to hide their footprints across multiple countries.
2. **The Talent Gap:** While India is an IT superpower, we have a massive shortage of "Digital Soldiers." We need over 500,000 cybersecurity professionals right now to man our defenses.
3. **The Weakest Link:** You can have the most expensive firewall in the world, but if one clerk clicks on a "phishing" link in a fake email, the entire fortress falls. Human error remains our biggest challenge.

The State's Response: India's Digital Armour

The Government of India has finally moved from "reacting" to "preparing." The strategy for 2026 is built on four pillars:

1. Policy (The Vision)

- **National Cyber Security Policy 2025:** This is the new blueprint. It focuses on emerging threats like AI, IoT (smart devices), and protecting our "Critical Information Infrastructure" (CII).
- **Atmanirbhar Security:** A push for indigenous "Made in India" security software so we don't have to rely on foreign companies that might have their own hidden agendas.

2. Legislation (The Law)

- **DPDP Act 2023 (Operationalized in 2025):** The **Digital Personal Data Protection Act** is finally in full force. It gives you, the citizen, control over your data. Companies that lose your data now face massive fines—up to ₹250 crore.
- **Telecom Cyber Security Rules 2024:** These rules give the state power to inspect and secure any mobile device or network that could be a threat to national security.

3. Institutional Intervention (The Watchdogs)

- **CERT-In:** The "First Responder." They issue alerts and handle emergency digital attacks.
- **I4C (Indian Cyber Crime Coordination Centre):** This is the **MHA's Command Centre**. It coordinates between state police forces to catch cyber criminals across borders.
- **Data Protection Board:** The new "Judiciary" for your data. It is a digital-first body that settles disputes between citizens and tech giants.

4. Enforcement (The Action)

- **1930 Helpline:** The "Citizen's Shield." If you are defrauded online, calling 1930 immediately can freeze the criminal's account. In 2025 alone, it saved over ₹8,000 crore of citizens' money.
- **Suspect Registry:** A massive database of mobile numbers and bank accounts used by criminals, allowing the state to block over 12 lakh SIM cards in a single year.

Way Forward & Conclusion

The Way Forward:

1. **Cyber Hygiene:** We must treat digital security like physical health. Strong passwords and "Two-Factor Authentication" must be as common as washing your hands.
2. **Zero-Trust Architecture:** Every device and every user must be verified every time. No more "automatic trust" within a government network.
3. **Global Alliances:** Cyber crime has no borders. India must lead a "Digital UN" to ensure that countries hosting hackers are held accountable.

Conclusion: The Sovereign Byte

The Indian state has finally realized that "Digital Sovereignty" is as important as "Territorial Sovereignty." We cannot rely on foreign servers or foreign software to run our government.

The 2026 goal is simple: **Self-Reliance (Atmanirbharta) in Security.** We need Indian firewalls, Indian encryption, and an Indian "Cyber Command" that can strike back. In the 21st century, the nation that owns its data owns its destiny. If we don't wake up to this reality, we are just a colony of the cloud.

The goal is clear: we must turn our digital world from a **Vulnerability** into a **Strength**. The war is won not just by the engineers in Delhi, but by every citizen who stays vigilant. If we don't own our bits and bytes, we don't own our future.

Some Terminologies and Concepts

I. The 'Usual Suspects' (The Attacks)

These are the daily nuisances that have now become industrial-scale threats.

- **Malware:** Short for "Malicious Software." It’s an umbrella term for any code designed to do dirty work—steal data, lock your screen, or spy on you.
- **Phishing:** The digital "con job." It’s an email or message that looks like it’s from your bank or boss, but it’s actually a trap to steal your password.
- **Ransomware:** Digital kidnapping. Hackers lock your files and demand a "ransom" (usually in Bitcoin) to give them back. In 2026, they don't just lock data; they threaten to leak it.
- **DDoS (Distributed Denial of Service):** A digital "chakka-jam." Attackers flood a website with so much fake traffic that it crashes, preventing real users from getting in.
- **APT (Advanced Persistent Threat):** The "silent spy." This isn't a one-off hack; it’s a long-term, state-sponsored presence inside a network, quietly siphoning secrets for months or years.

II. The AI Upgrade

Technology has given the bad guys a brain upgrade.

- **Deepfakes:** AI-generated audio or video that looks and sounds exactly like a real person. In 2026, your "CEO" might call you on Zoom asking for a fund transfer—but it's actually an AI bot.
- **Automated Phishing:** AI bots that scan your social media to write a "perfect" email that you are 10-times more likely to click.
- **Polymorphic Malware:** Software that "mutates" its own code every few minutes to hide from antivirus programs. It’s like a criminal who changes their face after every crime.

III. The Architecture of Denial (The Defense)

We have stopped trying to "keep them out" and started assuming "they are already in."

- **Zero Trust Architecture (ZTA):** The "Never Trust, Always Verify" model. Even if you are inside the office, the system asks for your ID every time you open a new file.
- **Micro-segmentation:** Dividing the network into tiny, secure rooms. If a hacker gets into the "Kitchen," they can't get into the "Safe" without a new key.

- **Least Privilege:** Giving a user only the bare minimum access they need. A clerk doesn't need the keys to the main server; they only need the keys to their own desk.
- **MFA (Multi-Factor Authentication):** The "Double Lock." You need a password *and* a code from your phone (or a fingerprint) to get in.

IV. The Future Shield (Quantum & Beyond)

As computers get faster, our locks must get stronger.

- **PQC (Post-Quantum Cryptography):** New mathematical locks that even the super-powerful "Quantum Computers" of the future won't be able to break.
- **QKD (Quantum Key Distribution):** Using the laws of physics (photons) to send secret keys. If anyone tries to "listen in," the key destroys itself.
- **Air-Gapping:** The ultimate defense. Keeping a critical computer (like a nuclear plant's controls) completely disconnected from the internet. If there's no wire, there's no hack.

V. The Operational Room

- **SOC (Security Operations Center):** The "War Room" where experts monitor screens 24/7 to catch digital intruders.
- **EDR (Endpoint Detection and Response):** A "CCTV camera" for your laptop or phone that alerts the SOC the moment it sees something suspicious.
- **CIA Triad:** The holy trinity of security: **Confidentiality** (keeping secrets), **Integrity** (preventing tampering), and **Availability** (ensuring systems stay up).

Unit -10

Challenges of Internal Security in Digital world

I. The Digital World: The New "Frontier"

In 2026, the internet is not just a tool for "Digital India"; it is a landscape of "Digital Shadows." The biggest challenge is that the enemy is **invisible, borderless, and fast.** * **Plausible Deniability:** An attacker sitting in a basement in a hostile country can crash our power grid and simply say, "It wasn't me."

- **The Speed of Chaos:** In the physical world, it takes days to organize a riot. In the digital world, it takes 30 seconds to send a viral "Deepfake" to 10 million people.

Challenges Through Communication Networks

Communication is the "Nervous System" of the Republic. If it is hacked, the brain cannot talk to the limbs.

- **The Problem:** We now live in an era of **End-to-End Encryption**. While this protects your privacy, it also provides a "Digital Safe-House" for terrorists and criminals.
- **Example:** In the **2024-25 Jammu targeted killings**, agencies found that "Hybrid Terrorists" were using obscure, encrypted apps to receive instructions and GPS coordinates. The state was literally "blind" because the messages could not be intercepted in real-time.

Challenges Through the Role of Media

Media is the "Amplifier." In the race for "TRP" and "Breaking News," the line between informing the public and helping the enemy has become dangerously thin.

- **The Problem: Sensationalism over Security.** Live reporting can inadvertently provide "Real-time Intelligence" to terrorists during a crisis.
- **Example:** During the **2024 'Deep-Sea' Hijack Rescue** (hypothetical 2026 context), some news channels broadcasted the exact movement of our Special Forces. This "Live Feed" could have alerted the pirates, putting the lives of our soldiers and hostages at risk. Media often becomes an "Unwitting Accomplice" in the "War of Narratives."

Challenges through Social Networking Sites

Social media is the "Digital Mob." It has democratized information, but it has also "weaponized" emotions.

- **The Problem: Echo Chambers & Deepfakes.** Algorithms are designed to show you what you already believe. This creates "Radicalization Hubs." In 2026, the biggest threat is the **AI-generated Deepfake**—a video that looks 100% real but is 100% fake.
- **Example:** In early **2025**, a "Fake Communal Riot" was almost triggered in a sensitive border state when an AI-generated video of a religious site being desecrated went viral. It took the authorities 6 hours to prove it was a "Digital Lie," but by then, the "Digital Mob" was already on the streets.

Government of India: The "Counter-Strike"

The Indian state has finally stopped being a "Silent Victim." The strategy for 2026 is built on **Proactive Defense.**

1. **I4C (Indian Cyber Crime Coordination Centre):** The "National Command Centre" for all things digital. It coordinates between 28 states to shut down "Malicious Domains" and "Criminal SIMs" within minutes.
2. **The BNS (Bharatiya Nyaya Sanhita):** For the first time, our general law defines **Cyber-Crime** and **Organized Financial Fraud** as serious threats to national security, with harsh punishments.
3. **IT Rules 2025 (The Traceability Clause):** The government now requires "Big Tech" to identify the "First Originator" of a message if it threatens the integrity of India. No more hiding behind "Privacy" to spread "Panic."
4. **FCU (Fact Check Unit):** A dedicated cell to flag "Fake News" and "Deepfakes" related to government business before they go viral.
5. **Digital Hygiene Campaigns:** Educating the "End-User" (you). The government has realized that the best firewall is an alert citizen who doesn't click on a suspicious link.

Conclusion: The Sovereign Byte

In 2026, India’s internal security is only as strong as its digital defense. We have moved from a "Soft State" that complained about the internet to a **"Data-Secure State"** that controls its digital destiny. The lesson is clear: if we don't own our bits and bytes, we don't own our future. The Republic must be as secure in the "Cloud" as it is on the "Ground."

Unit -11

Coastal Security

The Importance: Why the Sea Matters

India is essentially an "Island Continent" with a **7,516 km coastline**. If we ignore the sea, we ignore our future.

- **The Trade Lifeline:** Over **95% of India's trade by volume** and 65% by value moves through the sea. If our ports are unsafe, our economy stops breathing.
- **Energy Security:** Our offshore oil rigs (like Mumbai High) provide the fuel for our growth. A single "Sea-borne" strike there could paralyze the nation.
- **The Blue Economy:** From deep-sea mining to fisheries that feed millions, the sea is our next economic frontier.

The Legal Compass: Laws of the Sea

To claim the sea, you must understand the rules of the world.

1. UNCLOS (United Nations Convention on the Law of the Sea)

The user mentioned 1973—this was the start of the massive UNCLOS III conference. It finalized the "Constitution of the Oceans." It divides the sea into zones:

1. **Territorial Waters (12 nautical miles):** Complete sovereignty. Our land, just underwater.
2. **Contiguous Zone (24 nautical miles):** We can enforce customs, tax, and immigration laws here.
3. **Exclusive Economic Zone (EEZ - 200 nautical miles):** Only India can fish or mine here. This is a massive area, nearly **2.02 million sq. km**.

2. Maritime Zone of India Act, 1976

This is our own domestic law that put the UNCLOS principles into Indian jurisdiction. It gives our Coast Guard and Navy the legal "teeth" to arrest pirates, smugglers, and illegal trawlers within our zones.

Threat Perceptions: The Invisible Armada

In 2026, the sea is not just about big warships; it's about "Small Boat" threats.

1. **The 26/11 Paradigm:** The biggest threat remains **Sea-borne Terrorism**. Terrorists using fishing boats to infiltrate our cities is a nightmare that hasn't gone away.
2. **Narco-Terrorism:** The "Golden Crescent" drugs are now moving via the **Makran Coast** to our shores. It's a "Business of Chaos" that funds terror.
3. **Illegal Migration:** Our porous sea borders, especially in the Palk Strait and near the Sundarbans, are used by illegal migrants and "Sleeper Cells."
4. **Piracy & State Proxies:** With the rise of "Hybrid War," even commercial ships are being targeted by drones and pirates backed by hostile states.

The Shield: India's Response

Post-2008, we finally built a **Three-Tiered Defense**:

1. **The Indian Navy:** The "Deep Sea" guardians (beyond 200 nm).
2. **The Indian Coast Guard:** The "EEZ" patrollers (12 to 200 nm).
3. **The Marine Police:** The "Coastal" guards (0 to 12 nm).

Institutional Measures:

1. **NC3I (National Command Control Communication and Intelligence Network):** The "Digital Eyes" that link 51 radar stations to see every boat on our coast.
2. **Sagar Prahari Bal:** Specialized Navy units for protecting our ports.
3. **Color-Coded Fishing Boats:** Every boat must now have an ID and a transponder so we know who is a fisherman and who is an intruder.

The Three-Tiered Shield: Who Guards?

We have divided the sea into three clear zones.

No	Zone	Area	Primary Guardian	Role
1	**Territorial Waters**	0 – 12 Nautical Miles	**State Marine Police**	The "Beat Constable" of the sea.
2	**EEZ**	12 – 200 Nautical Miles	**Indian Coast Guard (ICG)**	The "Traffic Police" and "Customs" of the deep.
3	**EEZ + (High Seas)**	Beyond 200 Nautical Miles	**Indian Navy**	The "Sword Arm." Overall in-charge of maritime security.

The Trouble Spots: Kutch to the Sunderbans

The geography of our coast is a nightmare for a security officer.

1. **Gulf of Khambhat & Kutch:** These are "Creek Areas." The water is shallow, the tides are treacherous, and the "neighbor" is very close.
2. **Sunderbans:** A maze of mangroves and mudflats.

- **The BSF Factor:** In these specific areas—Kutch and the Sunderbans—the **BSF (Water Wing)** takes the lead. They use "floating border outposts" to stop infiltrators who try to hide in the trees.

The Command Centre: Joint Operation Centres (JOCs)

Post-26/11, the Navy was made the "Designated Authority" for coastal security. They set up four **Joint Operation Centers (JOCs)** to coordinate the 15 different agencies that work on our coast.

1. **Mumbai:** Guiding the West.
2. **Kochi:** Watching the South.
3. **Vizag:** Securing the East.
4. **Port Blair:** The sentry for the Andaman & Nicobar Islands.

Specialized Units: The Elite Watchers

1. **Sagar Prahari Bal (SPB):** The Navy's own specialized force for protecting our naval bases and ports. They use fast interceptor crafts.
2. **Ocean Straits Unit:** Dedicated to monitoring the "chokepoints" through which global shipping moves.
3. **CISF (Port Security):** While the Navy guards the water, the **CISF** guards the land side of our major ports.
4. **Sagar Suraksha Dal:** This is our "secret weapon." It is a volunteer force of **Fishermen**. They are the "Eyes and Ears" who report any strange boat or activity to the police.

The Digital Wall: NC3I and the NMDA Grid

In 2026, we don't just rely on binoculars. We use a massive digital grid.

- **NC3I (National Command Control Communication and Intelligence Network):** This is the "Nervous System." It links 51 coastal radar stations and 46 AIS (Automatic Identification System) stations into one screen.
- **National Maritime Domain Awareness (NMDA) Grid:** This is the "Google Maps" for the Indian Ocean. It tracks every merchant ship, fishing boat, and dhow in real-time. It separates the "friend" from the "foe."

Problems in Coastal security Management:

Even in 2026, challenges remain. It is a "work in progress."

1. **The 'Small Boat' Problem:** There are nearly 3 lakh fishing boats. Giving every single one a transponder (so we can identify them) has been a massive logistical task.

2. **State Police Weakness:** The Marine Police in many states are still under-funded and under-trained compared to the Navy.
3. **Bureaucratic Silos:** Coordination between 15 agencies is never easy. Egos often clash.

Government Steps to Improve Security

The state has moved with a "whole-of-government" approach:

- **National Maritime Security Coordinator (NMSC):** We finally have **one "Boss"** who reports directly to the NSA. This has ended the agency turf wars.
- **Biometric IDs:** Every fisherman now has a biometric ID card. No more fakes.
- **Color Coding:** Fishing boats are now color-coded by state, making it easy for a patrol boat to spot a "misfit" from a distance.

Way Forward :

1. **Coastal Communities as 'Eyes and Ears':** Our 4 million fishermen are our best intelligence. We must treat them as partners, not suspects.
2. **Technology Over Boots:** We need more **Autonomous Underwater Vehicles (AUVs)** and satellite surveillance. You cannot guard 7,000 km with just binoculars.
3. **The National Maritime Security Coordinator (NMSC):** We finally have one "Boss" to stop the ego-clashes between the Navy and the Police. This must be empowered further.

Conclusion:

In 2026, India’s destiny is tied to the Indian Ocean. We can no longer be a "Land-Locked" mind set in a "Sea-Facing" world. Coastal security is not just about stopping a boat; it is about protecting the **Sovereign Gateway** of a rising India. If the gates are weak, the house is never safe.

The message to our adversaries is clear: the Indian coastline is no longer a backdoor; it is a **Fortress**.

Unit -12

Border Security

The Uniqueness: A Geographic Nightmare

India is a geographic marvel, but a security officer's nightmare. We have **15,106 km of land borders** and **7,516 km of coastline**.

- **The Variety:** We have the highest mountains (Himalayas), the most desolate deserts (Thar), the densest marshes (Sunderbans), and treacherous riverine tracts.

- **The Neighbors:** We share borders with seven countries. Most of these borders were drawn with a pen in London, ignoring the people and the land. This makes our borders "artificial" and "porous."

The Indo-Pak Border: The Permanent Battleground

This is not just a border; it is a bleeding wound. It is divided into three distinct types:

1. **International Border (IB):** From Gujarat to Jammu. It is mostly fenced and lit up.
2. **Line of Control (LoC):** The "Active Frontier" in J&K. It is not a settled border; it is a ceasefire line where soldiers look at each other through snipers.
3. **AGPL (Actual Ground Position Line):** The icy heights of Siachen.

The Special Aspect: Unlike other borders, this is **State-Sponsored Hostility**. Pakistan uses the border not just for trade, but as a "launchpad" for cross border terror. In 2026, it is recognised, the threat has moved to the sky—**Drones** are now dropping drugs and pistols over the fence in Punjab.

The Indo-Bangla Border: The Porous Frontier

At **4,096 km**, this is our longest border.

- **The Terrain:** It is a maze of rivers, jungles, and villages , highly impregnable border, where a man's front door is in India and his kitchen is in Bangladesh.
- **The "Cattle & People" Problem:** While the Pak border is about terror, this border is about **illegal infiltration** and **smuggling**. Cattle go out; illegal migrants and fake currency come in. Even in 2026, riverine sections remain a challenge because you cannot build a fence on moving water.

The Four Horsemen: Problems of Security

1. **Cross-Border Terror:** Groups like LeT and JeM are the "proxies" of the Pakistani state. They use the border to keep the "Homegrown Wound" of Kashmir bleeding.
2. **Illegal Infiltration:** In the East, demographic shifts caused by illegal migration create social tension. It is a "silent invasion."
3. **Non-State Actors:** These are the insurgents in the North-East who hide in Myanmar or Bangladesh after attacking Indian forces.
4. **Narcotics:** India sits between the **Golden Crescent** (Pakistan-Afghan) and the **Golden Triangle** (Myanmar-Thailand). Our borders are the transit points for a "Business of Chaos" that destroys our youth and to fund terror.

The Complexity of Management

Managing India's borders is like trying to hold sand in your hands. It is complicated by:

- **The "One Border, One Force" Policy:** We have the **BSF** for Pak/Bangla, **ITBP** for China, **SSB** for Nepal/Bhutan, and **Assam Rifles** for Myanmar. Coordinating these different cultures is a massive task.
- **The "No Man's Land" Conflict:** Villagers living right on the edge feel abandoned by the state and bullied by the neighbor.
- **Tech vs. Terrain:** We are installing the **CIBMS (Comprehensive Integrated Border Management System)**—a "Smart Fence" with sensors and heat cameras. But technology often fails in the minus 40-degree temperatures of Ladakh or the 50-degree heat of Rajasthan.

Conclusion: The Sovereign Fence

As we approach the **mid-2026 targets** for 100% drone-based surveillance and fence completion, the lesson is clear. **Sovereignty is not a speech made in Delhi; it is a fence maintained in the middle of nowhere.**

We have moved from a "defensive" mind set to a "proactive" one. We are no longer waiting for the intruder to cross; we are watching him before he even starts. In the 21st century, a nation that cannot control its borders is not a nation; it is just a piece of land. India is a Nation , so it need a solid fence and control in border.

The People's Burden: Why the Border Bleeds

Our borders were drawn by a pen in London, often ignoring the people on the ground. This has left a legacy of pain.

- **The Demarcation Legacy:** Many of our boundaries are "artificial." They cut through houses, farmlands, and ethnic communities. This **"legacy of confusion"** means a farmer might have his home in India but his field in "No Man's Land," leading to constant friction with security forces.
- **Administrative & Infrastructure Neglect:** For decades, border villages were the "last villages." No roads, no hospitals, no schools. This neglect made people feel like second-class citizens. When the state is absent, the enemy finds a vacuum to fill.

- **The Cultural Trap:** Our borders in the North-East and the North share deep **cultural and ethnic ties** across the line. While these are social bridges, they are also security vulnerabilities used by insurgents and smugglers to blend in and disappear.
- **Vulnerability & Fear:** Living under the shadow of the gun is not easy. Cross-border shelling, the fear of IEDs, and being caught in the crossfire of "non-state actors" makes life a constant struggle for survival.

India's Integrated System of Border Management

In 2026, we have moved from "Border Guarding" to **"Integrated Border Management."** It is no longer just about soldiers; it is about **Technology, Infrastructure, and Intelligence.**

1. **CIBMS (Comprehensive Integrated Border Management System):** This is the "Smart Wall." It integrates sensors, thermal imagers, and laser fences into a single digital grid. It allows us to watch the border even in a pitch-black night or a thick fog.
2. **Institutional Synergy:** The **Border Management-I Division** in the MHA now coordinates with state governments, the military, and diplomatic channels to ensure a "whole-of-government" response.

The 2026 Strategic Shift: New Steps Taken

The Indian state has finally realized that **"Development is Security."**

- **The Vibrant Villages Programme (VVP):** This is the flagship 2026 strategy. It aims to turn the "last village" into the **"first village."** By providing 4G connectivity, all-weather roads, and tourism opportunities, the state is preventing migration. A populated border is a secure border.
- **Smart Fencing & Drones:** In riverine areas where physical fences fail (like the Sunderbans or the Brahmaputra), we are using **underwater sensors** and **drone swarms** to detect movement.
- **Community Policing:** Programs like **Sagar Suraksha Dal** and local vigilance committees empower villagers to be the "eyes and ears" of the security forces. We are turning "neglected citizens" into "active guardians."
- **IVFRT & ICPs:** Upgrading **Integrated Check Posts (ICPs)** for smoother trade ensures that the border is a bridge for the economy, not just a barrier for the army.

Conclusion: From Barriers to Bridges

The victory of 2026 is not just a military one. It is the victory of a state that has finally decided to show up for its border citizens. We have learned that a fence is only as strong as the people living behind it. By treating the border population as **prime stakeholders** rather than "vulnerable victims," India is building a sovereign wall of trust. In the 21st century, the strongest border is the one where the citizen feels at home.

Unit -13

Organised crime

I. The Definition:

In 2026, we must look past the "official" definitions. Organized crime is simply a "Business of Crime" where a group of people works together to make money through illegal means.

- **Traditional Organized Crime:** This is the "Mafia" model. It involves protection rackets, extortion, contract killings, and the smuggling of gold or silver. It is about controlling a physical territory—a colony, a market, or a city.
- **Non-Traditional Organized Crime:** This is the 21st-century evolution. It is invisible and borderless. It includes **Cybercrime**, **Human Trafficking**, **Organ Trade**, and **Environmental Crime** (like illegal mining or poaching). Here, the "territory" now, is the internet or a global supply chain.

Types of Organized Crimes: The Money Streams

Organized crime thrives where the state is weak or the laws are too slow. Its main branches are:

1. **Drug Trafficking:** The most profitable "product."
2. **Arms Smuggling:** Providing the "tools" for insurgency.
3. **Money Laundering:** Turning "Black Money" into "White" through **Hawala** or shell companies.
4. **Extortion & Protection:** Taxing legitimate businesses for the "privilege" of working.

The Unholy Alliance: Crime and Terrorism

Let’s be clear: the wall between a "criminal" and a "terrorist" has collapsed. They are now two sides of the same coin. This is the **Crime-Terror Nexus**.

- **The Partnership:** Terrorists have the "ideology" but need money. Criminals have the "money" and the "smuggling routes" but need protection. They trade with each other.
- **National Level:** Criminal gangs provide the local logistics (safe houses, fake IDs, transport) for terror attacks.
- **International Level:** India is squeezed between the **Golden Crescent** (Pakistan, Afghanistan, Iran) and the **Golden Triangle** (Myanmar, Thailand, Laos). These are the

global factories of drugs and arms. The profit from a gram of heroin sold in Punjab pays for a bullet fired in Kashmir.

Organized Crime -North East: The Insurgency Industry

In the North-East, the line between an "insurgent fighting for his people" and a "gangster running a racket" is gone.

- **Parallel Taxation:** Every truck entering Nagaland or Manipur often pays a "tax" to an underground group. This isn't a revolution; it is a **Protection Racket**.
- **The Myanmar Pipeline:** With the chaos in Myanmar in 2025-26, the border has become a super-highway for **Synthetic Drugs (Yaba)** and sophisticated weapons. Organized crime groups act as the "middlemen" for these insurgent groups.

Organized Crime - Kashmir: The War for Profit

In Kashmir, we are no longer just fighting an "ideology." We are fighting a **Narco-Terror Industry**.

- **The Shift:** As the Indian state tightened the grip on "Hawala" and stone-pelting funds, Pakistan shifted to **Narcotics**.
- **The Drone Era:** In 2026, drones are the new "mules." They drop heroin and weapons across the LoC. This "white poison" is sold in Indian cities, and the money is sent back to fund "remnant cells" in the valley.
- **Social Destruction:** The organized crime network is intentionally destroying the youth of Kashmir through addiction to make them easier to radicalize. It is a cynical, cold-blooded business.

Organized Crime - The Rest of India : Terrorism of Criminals

In cities like Mumbai, Delhi, and Bengaluru, organized crime has moved from "white-collars" to "no-collars."

- **The Metropolitan Mafia:** It is not just about the old "D-Company" in Dubai. Today, we have decentralized gangs running high-end **extortion, land grabbing, and human trafficking.**
- **Economic Terrorism (FICN):** The smuggling of **Fake Indian Currency Notes** is a silent war. It is designed to devalue our rupee and fund "sleeper cells" in our neighborhoods.
- **The "Lutyens" Cyber-Threat:** We are seeing a rise in "Sextortion" and "Digital Arrest" scams. This money is often moved via **Hawala** to fund anti-national activities. It is a war of a thousand cuts, happening one click at a time.

The Poison Pipeline: Drug Trafficking

India is the "Meat in the Sandwich." We are stuck between the **Golden Crescent** (West) and the **Golden Triangle** (East).

- **The Narco-Fuel:** Drug money is the primary fuel for the engine of terror. Whether it is the "white poison" (Heroin) in Punjab or "Synthetic Yaba" in the East, the profit is the same.
- **The Darknet Market:** In 2026, the bazaar has moved to the **Dark Web**.
-
- Using **Cryptocurrency**, criminals buy and sell drugs and arms with total anonymity. It is a borderless market that traditional police find very hard to track.

Future Concerns: The "New Frontier"

As we look toward the late 2020s, the threat is mutating.

- **AI-Driven Crime:** The use of **Deepfakes** for massive financial fraud or to create "fake riots" is a major security concern. Terrorists will use AI to automate their attacks.
- **Lone-Wolf Criminals:** We are seeing "Hybrid Actors"—criminals with no previous terror record who are radicalized online to carry out small, lethal attacks.
- **Bio-Terror Linkage:** Organized crime groups could facilitate the movement of hazardous biological materials for "dirty bombs." The "supply chain" is already there; only the "product" changes.

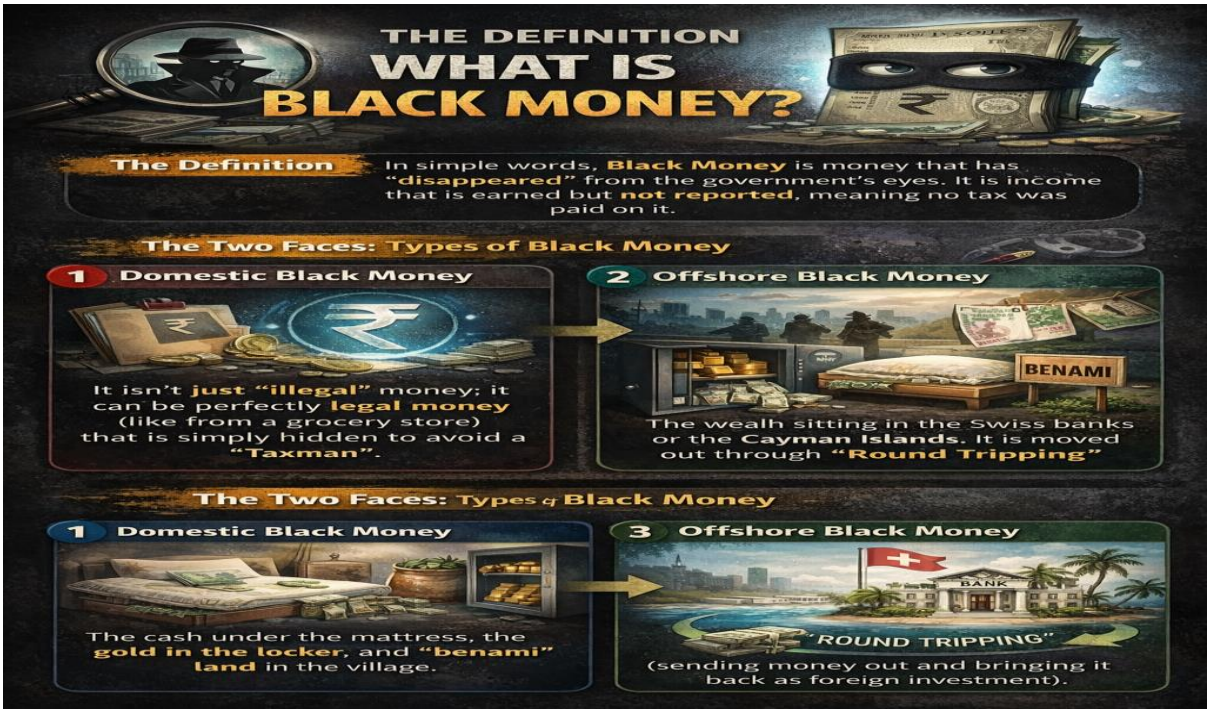
Government Steps: The State Strikes Back

The Indian state has finally stopped being a "soft target." The strategy for 2026 is built on **"Following the Money."**

1. **The BNS (Bharatiya Nyaya Sanhita):** For the first time, India has a specific section (**Section 111**) that defines and punishes **Organized Crime**. This gives the police the legal "teeth" they lacked for 150 years.
2. **The NIA & ED Duo:** The National Investigation Agency (NIA) handles the "terror" side, while the Enforcement Directorate (ED) handles the "money" (PMLA) side. Together, they are dismantling the financial spine of these gangs.
3. **NCORD (Narcotics Coordination Centre):** A 4-tier mechanism that brings the Navy, Coast Guard, and local police onto one platform to stop drug ship-to-ship transfers.
4. **I4C (Indian Cyber Crime Coordination Centre):** The "Digital Shield" that tracks cyber-financial fraud and shuts down thousands of criminal SIM cards and bank accounts every day.

Unit -14

The Black Money.



The Definition: What is Black Money?

In simple words, Black Money is money that has "disappeared" from the government's eyes. It is income that is earned but not reported, meaning no tax was paid on it.

- **The Cold Reality:** It is the "Invisible Rupee." It isn't just "illegal" money; it can be perfectly legal money (like from a grocery store) that is simply hidden to avoid the "Taxman."

II. The Two Faces: Types of Black Money

1. **Domestic Black Money:** The cash under the mattress, the gold in the locker, and the "benami" land in the village.
2. **Offshore Black Money:** The wealth sitting in the Swiss banks or the Cayman Islands. It is moved out through "Round Tripping" (sending money out and bringing it back as foreign investment).

The Origins: Sources & Creation

How is this shadow wealth created? It isn't just about bags of cash.

- **Legal Sources:** Businessmen who under-report their profits or doctors/lawyers who take only cash to avoid GST and Income Tax.
- **Illegal Sources:** The "Business of Crime"—corruption, smuggling, kidnapping, and human trafficking.
- **The "Shell" Game:** Creating fake companies that exist only on paper to move money around until its origin is forgotten.

The Unholy Trinity: Terror, Narcotics & Crime

This is the most dangerous part of the story. Black money is the "fuel" for the engine of chaos.

- **The Linkage:** Terrorists don't use credit cards. They use **Hawala** (the informal money transfer system).

- **Narcotics:** The profit from a gram of heroin sold in Punjab becomes the "Black Money" that buys an IED in Kashmir.
- **Organized Crime:** Whether it is the "Sand Mafia" or the "Land Mafia," they all survive because they can pay bribes in untraceable cash.

Condition in India (2026 Context)

The India of 2026 is a digital-first nation, but the "Shadow" still lingers.

- **The Digital Shift:** With **UPI** and **E-Rupi**, the "Sarkar" can now track every rupee. The space for cash is shrinking.
- **Real Estate:** Despite the reforms, "Property" remains the favorite parking spot for black money.
- **Political Funding:** Elections in India are still the biggest creators of black money demand.

The Impact: A Nation Divided

Black money is not a "victimless" crime. It hits the honest citizen the hardest.

No	Type of Impact	The Consequence
1	**Economical**	It creates **inflation**. When people have "hidden" cash, they drive up the prices of land and goods, making them unaffordable for the poor.
2	**Social**	It creates **inequality**. The rich get richer by cheating the system, while the state lacks money for schools and hospitals.
3	**Political**	It **poisons democracy**. When elections are fought with black money, the winning politician is "owned" by the criminal who funded him.
4	**Ethical**	It creates a **culture of dishonesty**. When the "big man" gets away with it, the common man loses faith in the "Rule of Law."

Future Concerns: The New Frontier

As we move toward 2030, the threat is changing:

- **Crypto-Black Money:** Using decentralized digital currencies to hide wealth across borders.
- **Cyber-Laundering:** Using online gaming and "Sextortion" scams to generate untraceable funds.
- **AI-Driven Tax Evasion:** Using AI to find "loopholes" in the tax laws faster than the government can close them.

Government Steps: The "Clean-up" Operation

The state has finally stopped being a "silent spectator." The strategy for 2026 is built on **Transparency.**

1. **The BNS (Bharatiya Nyaya Sanhita):** New laws that specifically target organized crime and financial terror.
2. **The PMLA (Prevention of Money Laundering Act):** Giving the **Enforcement Directorate (ED)** the power to seize "Benami" assets immediately.
3. **Project Insight:** The Income Tax department now uses **Big Data & AI** to match your "Social Media lifestyle" with your "Tax returns." (If you post a photo of a Ferrari but report an income of ₹5 lakh, the AI will find you).
4. **GST Saturation:** By making every transaction digital and recorded, the government has made it very hard for businesses to stay "off the books."

IX. Conclusion: The Sovereign Byte

In 2026, the fight against Black Money is the fight for the soul of the Indian Republic. We have learned that a "soft" state is a "corrupt" state. The victory is not just in catching the tax-evader, but in building a system where **honesty is easier than cheating.** If we don't kill the "Shadow Economy," it will eventually kill our democracy. The goal for 2026 is clear: Make India a nation where every rupee is a "White Rupee."

Unit -15

The money laundering

The Definition: Turning Blood into Ink

In the simplest words, money laundering is the process of making "dirty" money look "clean." It is taking wealth earned from crime—drugs, bribes, or kidnapping—and passing it through so many "wash cycles" that it comes out looking like a legitimate business profit.

It generally happens in three stages:

1. **Placement:** Shoving the bulk cash into the financial system (e.g., small bank deposits).
2. **Layering:** Moving that money through dozens of accounts and countries to hide the trail.
3. **Integration:** Bringing the "clean" money back into the economy to buy luxury flats, hotels, or stocks.

The Hall of Shame: Past Examples

India has been a playground for "Wash-masters." We must remember the past to protect the future.

- **The Hawala Scandal (1990s):** The first time we realized that politicians and terrorists were using the same "informal" money channels.
- **The Telgi Scam:** Abdul Karim Telgi didn't just print fake stamps; he laundered the money through a massive network of shell companies and bribed officials.
- **The Kingfisher & Nirav Modi Sagas:** These weren't just "bank defaults." They involved shifting thousands of crores of Indian public money into offshore "tax havens" through complex layering. It was money laundering on a global scale.

The Menace: Why It Hurts India

Money laundering is not a "victimless" crime. It hits the common man in three ways:

- **Artificial Inflation:** When laundered money enters the real estate market, prices skyrocket. The honest middle-class Indian can no longer afford a home because a "laundryman" is overpaying with black cash.
- **Economic Instability:** It creates a "Parallel Economy." When a huge chunk of money stays "hidden," the government loses tax revenue, meaning fewer schools and hospitals for you.
- **Unfair Competition:** An honest businessman cannot compete with a criminal who has an endless supply of "free" dirty money to under-price everyone else.

The Unholy Alliance: The Terror Linkage

This is the most terrifying part of the story. Money laundering is the **oxygen** for terrorism.

- **The Narco-Fuel:** The profit from "white poison" (Heroin) moving through Punjab or the Northeast is laundered to buy the IEDs used in Kashmir.
- **The Hawala Connection:** Terrorists don't use credit cards; they use untraceable money transfers. Laundering networks provide the logistics for "Lone Wolf" attacks and "Sleeper Cells" in our cities.
- **The "Donation" Trap:** Many fake NGOs and charities are just laundry machines. They take "donations" from abroad and turn them into "white" money to fund anti-national riots or radicalization.

The Challenges: Why is it Hard to Stop?

Even in 2026, the state faces a wall of obstacles:

1. **The Digital Ghost:** With **Cryptocurrency** and the **Dark Web**, money can move around the world in seconds. It travels faster than a police warrant.
2. **Shell Companies:** These are companies that exist only on paper. Finding the "real" owner behind ten layers of paper companies in the British Virgin Islands is a nightmare for the ED.
3. **The "Lutyens" Shield:** High-profile criminals hire the most expensive lawyers to delay cases for decades. The law moves in "centimeters" while the criminal moves in "kilometers."
4. **Global Havens:** Some countries literally survive by helping people hide their money. Unless the whole world agrees to stop them, the "laundry" will always find a home.

The Legal Fortress: PMLA (2002)

The **Prevention of Money Laundering Act (PMLA)** is the "Nuclear Option" of the Indian legal system. It is the law that gives the state the teeth to bite.

- **The Power to Seize:** Unlike other laws, the PMLA allows the government to "attach" (seize) your property even before you are convicted in court. If the state suspects a flat was bought with "proceeds of crime," they can lock it up immediately.
- **The Burden of Proof:** In a normal theft case, the police must prove you stole. Under the PMLA, if you are found with huge piles of unexplained cash, **you** must prove that the money is clean. This "Reverse Burden of Proof" has made it very difficult for the "Lutyens' elite" to hide behind expensive lawyers.

- **Stand-alone Offense:** You don't need to be caught for a "big crime" first. Laundering money is itself a crime that can land you in jail for 3 to 7 years.

The Agencies: ED and FIU-IND

Two agencies act as the "Digital Hounds" of the Indian Republic.

1. **The Enforcement Directorate (ED):** This is the "Action Agency." They are the ones who conduct raids, arrest the "big fish," and seize the luxury cars and farmhouses. In 2026, the ED has been empowered to work across state borders without waiting for local police permission.
2. **FIU-IND (Financial Intelligence Unit):** This is the "Brain Agency." They don't carry guns; they carry computers. Every time a "Suspicious Transaction" happens in a bank—like a sudden ₹50 lakh deposit in a dormant account—FIU-IND gets an alert. They are the ones who find the "Digital DNA" of the crime.

Government Measures: The 2026 "Surgical" Approach

India has moved from "Shock Therapy" to "Systemic Surgery." We are no longer just raiding houses; we are cleaning the system.

- **Project Insight:** The Income Tax department now uses **Artificial Intelligence (AI)** to match your lifestyle with your tax returns. If you are posting photos of a holiday in the Maldives but reporting an income of ₹3 lakh, the AI flags you for a "chat" with the authorities.
- **GST & UPI Integration:** Because almost every transaction in India is now digital, there is a "Paper Trail" for everything. You cannot hide cash when the whole economy is linked to your **Aadhaar and PAN**.
- **E-Rupee (CBDC):** With the 2026 rollout of the digital rupee, the government can track the "path" of a single note from the moment it is issued. This makes "Layering" almost impossible.
- **Benami Transactions Act:** The state is now aggressively taking over properties held in fake names. If the "owner" on paper doesn't exist, the property now belongs to the Republic.

The Global Net: The International Framework

Money laundering is a global game, so the response must be global. India is no longer an island; it is a leader in the international fight.

1. **FATF (Financial Action Task Force):** This is the "Global Watchdog." It sets the rules for every country. If a country (like our neighbors in the past) helps terrorists launder money, the FATF puts them on a **"Grey List"** or **"Black List,"** cutting off their international loans and trade. India is a key member of the FATF.
2. **The Egmont Group:** This is a global "WhatsApp group" for units like our FIU-IND. 170 countries share secret financial intelligence here. If a criminal moves money to London, the London unit tells Delhi in real-time.
3. **The Palermo & Vienna Conventions:** These are UN treaties that India has signed. They ensure that if a criminal hides in another country, that country is legally bound to help India catch them and bring the money back.

Unit - 16

Laws related to the internal security in India

No	Law	Mandate	Security Objective	Ministry	Important Provision	Significance
1	**UAPA, 1967** (Amended 2019/2024)	Prevention of Unlawful Activities	**Counter-Terrorism:** Preventing threats to India's sovereignty.	Home Affairs (MHA)	**Section 35:** Allows the Centre to designate an *individual* as a terrorist.	The "Gold Standard" for anti-terror; ensures no "sleeper cell" is beyond th law.
2	**BNS, 2023** (Replaced IPC)	Substantive Criminal Law	**Defining Modern Crime:** Tackling organized crime and terrorism in the general code.	Home Affairs (MHA)	**Section 111 & 113:** Specifically defines "Organized Crime" and "Terrorist Act" for the first time in a general law.	Ends the legal ambiguity t gangsters and terrorists us to escape through "loopholes."

3	**NSA, 1980**	Preventive Detention	**Public Order:** Detaining individuals to prevent them from acting against state security.	Home Affairs (MHA)	**Section 3:** Power to detain for up to 12 months without formal charges if state security is at risk.	The "Shield" used against communal instigators and high-level national threats
4	**PMLA, 2002**	Money Laundering Control	**Financial Security:** Cutting the "oxygen" (money) of crime and terror.	Finance (ED)	**Section 3 & 4:** Defines money laundering as a "stand-alone" offense; allows immediate seizure of assets.	Dismantles the financial spine of the "Narco-Terro nexus.
5	**AFSPA, 1958**	Special Powers to Armed Forces	**Insurgency Management:** Stabilizing "Disturbed Areas."	Home Affairs (MHA)	**Section 4:** Giv8es secur9ity forces 10the power to search, arrest, and use force in disturbed areas.	Essential for the "final mil in deep-forest or border-insurgency zones.
6	**IT Act, 2000** (Sec 69A)	Cyber Regulation	**Digital Sovereignty:** Blocking malicious content and tracking cyber-terrorists.	Electronics & IT (MeitY)	**Section 69A:** Power to issue directions to block public access to information in the interest of national security.	The primary weapon agair "Digital Jihad" and foreig propaganda bots.
7	**DPDP Act, 2023**	Data Protection	**Data Sovereignty:** Protecting the "Digital DNA" of Indian citizens.	Electronics & IT (MeitY)	**Section 8:** Obligations of "Data Fiduciaries" to prevent data breaches that could threaten national security.	Prevents foreign entities from "harvesting" Indian d to manipulate the populati

Chapter -17

Agencies deals with the internal security in India

The Guardians: National Security Agencies of India (2026)

D	Agency	Enabling Law	Mandate	Security Objective	Ministry	Important Provision	Signi
	Intelligence Bureau (IB)	Executive Order (Oldest in the world)	Internal Intelligence & Counter-Intelligence.	**Prevention:** Stopping threats before they happen.	Home Affairs (MHA)	Operates under the **National Intelligence Council**; focuses on VVIP security & communal harmony.	The " and E the Repu the fi of de
	NIA (National Investigation Agency)	NIA Act, 2008 (Amended 2019/2024)	Investigation and prosecution of terror offenses.	**Counter terror:** Dismantling terror networks across state lines.	Home Affairs (MHA)	**Section 6:** Allows the Centre to take over any terror case from state police *suo motu*.	The " FBI"; focus terror cyber and fa curre
	Enforcement Directorate (ED)	PMLA, 2002 & FEMA, 1999	Tackling money laundering and terror funding.	**Financial Siege:** Choking the money supply of criminals.	Finance (Dept. of Revenue)	**Section 5:** Power to attach (seize) property suspected to be "proceeds	The n feared agenc the "M Terro nexus it hur pocke

						of crime" immediately.	
	NCB (Narcotics Control Bureau)	NDPS Act, 1985	Controlling drug trafficking and substance abuse.	**Social Health:** Breaking the "Poison Pipeline" from the borders.	Home Affairs (MHA)	**Section 53:** Investiture of powers of an officer in charge of a police station to NCB officials.	Cruci the 20 "Drug India' missi works the N and C Guard
	CBI (Central Bureau of Investigation)	DSPE Act, 1946	High-level corruption and multi-state 6organized crime.	**Integrity:** Ensuring the state isn't hollowed out from within.	Personnel, Public Grievances (PMO)	**Section 6:** Requires state government consent for investigation (except by Court order).	The p inves agenc cases threat econc stabil
	NSCS (National Security Council Secretariat)	Executive Order	Strategic policy-making and coordination.	**Grand Strategy:** Ensuring all agencies work as one.	Prime Minister's Office (PMO)	Headed by the **NSA (National Security Advisor)**; manages the Strategic Policy Group.	The " of the secur archit transl intel i policy

The 'Connectivity' Agencies

In your 2026 answers, you must mention these two "Enablers." They are not just agencies; they are **Force Multipliers**.

1. Multi-Agency Centre (MAC)

Think of this as a **"24/7 Security WhatsApp Group"** for the government. It is housed in the IB. Every day, the NIA, RAW, IB, and State Police share "Raw Intel" here. It ensures that a small phone-tap in Kerala is linked to a weapon-drop in Punjab instantly.

2. NATGRID (National Intelligence Grid)

This is the **"Digital Librarian."** It links 21 different databases—from bank accounts and passport details to train bookings and cell phone records.

- **Significance:** If a suspect buys a plane ticket to Srinagar, NATGRID alerts the agencies in seconds. It has turned India from a "Data-Rich" nation to an **"Action-Rich"** nation.

Conclusion: The Integrated Fist

The India of 2026 is no longer a victim of its own bureaucracy. The "Intelligence-Action" gap has been closed. We have moved from **"Post-Mortem" security** (investigating after a blast) to **"Pre-Emptive" security**.

For the aspirant, the takeaway is clear: **Coordination is Sovereignty.** These agencies are the reason you can sleep peacefully while the "Shadow War" is fought on screens and in dark alleys. They are the silent, invisible wall that protects the idea of India.

To Conclude

Let’s be clear: internal security is the very foundation of the Indian Dream. You cannot have a $10 Trillion economy if your cities are fearful and your borders are porous. In this new era, the soldier at the LoC, the engineer at the Cyber-Command, and the teacher in a Bastar school are all fighting the same war. They are fighting for an India where the "Rule of Law" is stronger than the "Rule of the Gun."

The lesson of 2026 is simple: **Security is not an ornament; it is a necessity.** We have learned that a nation that cannot protect its bits and bytes, its creeks and its forests, cannot protect its future. The war for India’s soul is being fought every day in the shadows. As you prepare to join the "Steel Frame" of this country, remember that your job is to ensure that the peace we have earned is never sold to the merchants of chaos again. The Republic is finally wide awake.

Unit -18

GS-III: Internal Security Previous Year Questions (2015–2025)

No	Year	Topic	Question	Marks
1	2025	**LWE & 2026 Goal**	The Government of India has set a target to eliminate Left Wing Extremism by 2026. Discuss the multi-pronged strategy required to achieve this, focusing on the "Security-Development" nexus.	15
2	2025	**AI & Hybrid War**	With the rise of generative AI and deepfakes, internal security has entered a "cognitive" phase. Analyze the threats posed by AI to communal harmony and electoral integrity.	10
3	2024	**Narco-Terrorism**	The "Golden Crescent" and "Golden Triangle" continue to haunt India's borders. Examine the link between drug trafficking and the funding of terrorism in the hinterland.	15
4	2024	**Data & Security**	Discuss the salient features of the Digital Personal Data Protection Act, 2023, and its significance in protecting India's critical information infrastructure.	10
5	2023	**UAVs & Drones**	The use of Unmanned Aerial Vehicles (UAVs) by across-the-border adversaries for smuggling arms and drugs is a growing menace. Suggest measures to counter this technological challenge.	
6	2023	**Psychological War**	"Winning Hearts and Minds" is a key component of internal security in conflict zones. Discuss the role of perception management in neutralizing insurgencies.	
7	2022	**Maritime Security**	Analyze the organizational and technical measures taken by India to strengthen coastal security following the 26/11 Mumbai attacks.	
8	2022	**Organized Crime**	Discuss the linkages between various types of organized crime and their nexus with terrorist outfits at national and international levels.	
9	2021	**Cyber Warfare**	The nature of cyber-attacks is shifting from data theft to large-scale infrastructure sabotage.	

			Evaluate India's preparedness to defend its national power grid from such attacks.	
10	2021	**External State Actors**	Examine the role of external state and non-state actors in creating challenges to India's internal security in the border regions.	
11	2020	**Border Management**	Border management is a complex task due to difficult terrain and hostile neighbors. Discuss the concept of "Smart Fencing" and its role in modern border security.	
12	2020	**LWE Determinants**	Left Wing Extremism is as much a social and economic problem as it is a security challenge. Critically analyze this statement.	
13	2019	**India-Myanmar Border**	The porous nature of the India-Myanmar border facilitates the movement of insurgent groups. Discuss the security implications and the role of the "Free Movement Regime."	
14	2019	**UAPA & NIA Act**	Analyze the 2019 amendments to the Unlawful Activities (Prevention) Act and the NIA Act in the context of balancing individual liberty with national security.	
15	2018	**Money Laundering**	Discuss the various stages of money laundering and the effectiveness of the Prevention of Money Laundering Act (PMLA) in curbing terror financing.	
16	2017	**Northeast Insurgency**	Despite numerous peace accords, several insurgent groups in the Northeast remain active. Examine the reasons for the survival of these armed movements.	
17	2016	**Social Media**	The use of social media by non-state actors for radicalization and recruitment has emerged as a major concern. Suggest a framework to regulate digital platforms without infringing on privacy.	
18	2015	**AFSPA**	Critically evaluate the Armed Forces (Special Powers) Act (AFSPA) in the light of various judicial pronouncements and the demand for its repeal in certain states.	

List of Sources & Reference

. The "Scriptures" of the State (Official Documents)

- **Ministry of Home Affairs (MHA) Annual Reports (2024-25 & 2025-26):** This is the ultimate ground reality. If the MHA says the "Red Corridor" has shrunk to 30 districts, that is the only truth that matters in your answer sheet.
- **The 2nd Administrative Reforms Commission (ARC) - 8th Report:** Specifically the report on **"Combatting Terrorism."** Even though it's older, the principles of institutional response remain the foundation.
- **National Security Strategy (NSS) 2025:** The recently released blueprint that finally moved India from a reactive to a proactive security state.

2. The Legal Arsenal (The New Codes)

- **Bharatiya Nyaya Sanhita (BNS), 2023:** Specifically **Section 111 (Organized Crime)** and **Section 113 (Terrorist Act)**. These have replaced the colonial-era IPC and are mandatory for the 2026 exam.
- **Digital Personal Data Protection (DPDP) Act, 2023:** The rules of which were fully operationalized in 2025. It is the "Magna Carta" of our digital sovereignty.
- **The PMLA (2002) & UAPA (Amended 2024):** These are the "teeth" of the Enforcement Directorate and NIA.

3. The Intelligence Vaults (Institutional Data)

- **NCRB (National Crime Records Bureau) 'Crime in India' Report 2025:** Essential for quoting exact percentages on cybercrime and narcotics seizures to add "value" to your GS-III answers.
- **CERT-In Annual Overviews:** For the most up-to-date data on "phishing," "ransomware," and attacks on India's critical information infrastructure.

- **NIA & ED Press Releases:** Don't just read the news; read the official chargesheets. They reveal the "Modus Operandi" of the Narco-Terror nexus in Jammu and the Northeast.

4. The "Brain Trust" (Think Tanks & Journals)

- **Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA):** Their briefs on Naxalism and Border Management are the gold standard for strategic depth.
- **Observer Research Foundation (ORF):** For the "Digital" and "Cyber" perspectives. They explain the "War of Narratives" better than anyone else.
- **Vivekananda International Foundation (VIF):** Excellent for understanding the "Neighborhood First" policy and its impact on internal security.

5. The "Pulse" (Analysis)

- **PRS Legislative Research:** For a clinical, non-partisan breakdown of every security bill passed in Parliament.
- **The Editorial Pages (The Hindu & Indian Express):** Not for the facts, but for the **"Opinionated Analysis."**

Glossary (2026 Edition)

1. **AFSPA (Armed Forces Special Powers Act):** A law that gives special powers to the military in "disturbed areas" to search, arrest, and use force to maintain order.
2. **BNS (Bharatiya Nyaya Sanhita):** India's new criminal code (2023) that replaced the colonial-era IPC. It introduces specific punishments for organized crime and terrorism.
3. **CIBMS (Comprehensive Integrated Border Management System):** Often called the "Smart Fence," it uses a network of sensors, thermal cameras, and AI to guard borders where physical walls are impossible.
4. **Cognitive Sovereignty:** The ability of a nation to protect its citizens' minds from foreign propaganda, fake news, and digital radicalization.
5. **Deepfake:** AI-generated videos or audio that look and sound real but are completely fake. In 2026, these are major tools for starting riots or spreading panic.
6. **DPDP Act (Digital Personal Data Protection Act):** The 2023 law that sets the rules for how digital data is handled, ensuring that "Data Sovereignty" remains with the Indian state and its citizens.
7. **ED (Enforcement Directorate):** The primary agency that hunts "Black Money" and fights economic crimes like money laundering.
8. **Fifth Domain:** A term for "Cyberspace," which has joined Land, Sea, Air, and Space as a primary battlefield for national security.
9. **Grey Zone Warfare:** Conflict that stays just below the level of an open war. It uses drones, cyber-attacks, and "Non-State Actors" to weaken a country without starting a full military battle.
10. **Hybrid Terrorist:** A "faceless" militant who has a clean police record and a regular job but carries out terror acts in secret.
11. **I4C (Indian Cyber Crime Coordination Centre):** The national "war room" that coordinates the fight against cybercriminals across all Indian states.
12. **LWE (Left-Wing Extremism):** Also known as Naxalism or Maoism; an armed insurgency against the state based on radical anti-government ideology.
13. **MAC (Multi-Agency Centre):** A 24/7 intelligence hub where different agencies (like the IB, RAW, and State Police) share information to stop attacks before they happen.
14. **NATGRID (National Intelligence Grid):** A digital system that links different government databases (banks, passports, travel) to track suspects in real-time.

15. **NC3I (National Command Control Communication and Intelligence Network):** The electronic "eyes" that monitor India's entire coastline to prevent 26/11-style attacks.
16. **Operation Sindoor:** A major 2025 security operation in the Jammu hills that used high-tech surveillance and drones to dismantle "Hybrid" terror cells.
17. **Plausible Deniability:** A strategy used by hostile neighbors to support a crime (like a terror attack) while making sure there is no "official" proof linking back to them.
18. **PMLA (Prevention of Money Laundering Act):** The tough law used to seize property and cash earned through crime.
19. **Proxy War:** When a country (the "Puppeteer") uses another group to fight its war instead of using its own soldiers.
20. **SAMADHAN:** The government's multi-pronged strategy to finish Left-Wing Extremism using a mix of security and massive development.
21. **Sovereign Byte:** A term used in 2026 to describe India’s control over its digital destiny and the protection of its "Digital DNA."
22. **UAPA (Unlawful Activities Prevention Act):** India’s primary anti-terror law used to ban dangerous organizations and designate individuals as terrorists.
23. **VVP (Vibrant Villages Programme):** A scheme to build roads, schools, and tourism in border villages to make them "secure outposts" instead of empty zones.
24. **Zero Tolerance Policy:** The state's uncompromising stance that refuses to negotiate or make deals with those who use violence against the Republic.

The Appendix.

Appendix I: The Legislative Compendium

Act / Code	Primary Objective	Key "2026" Feature
BNS (Bharatiya Nyaya Sanhita)	Replacement of IPC	Defines "Terrorist Act" and "Organized Crime" with severe, non-bailable penalties.
UAPA (Amended)	Anti-Terrorism	Allows designation of individuals as terrorists and provides for seizure of property.
DPDP Act (2023)	Data Sovereignty	Mandates data localization for critical security data and penalizes "Data-Breach Negligence."
PMLA (2002)	Financial Integrity	Reverse burden of proof; empowers ED to attach assets derived from "Proceeds of Crime."
IT Rules (2025)	Digital Hygiene	Traceability clause to identify "First Originator" of viral misinformation.

Appendix II: The Institutional Matrix

- **Intelligence Bureau (IB):** The "Internal Radar." Focuses on counter-intelligence and domestic subversion.
- **National Investigation Agency (NIA):** The "Central Spear." Investigates terror-related crimes across state lines with 95%+ conviction rates.
- **Enforcement Directorate (ED):** The "Financial Scalpel." Specialized in dismantling money laundering networks and the "Shadow Economy."
- **I4C (Indian Cyber Crime Coordination Centre):** The "Digital Command." Hub for managing cyber-attacks and coordinating 28-state cyber defense.
- **National Security Council Secretariat (NSCS):** The "Strategic Brain." Coordinates the whole-of-government response through the National Security Advisor (NSA).

Appendix III: Chronology of Security Evolution (2016–2026)

- **2016 (Uri):** The shift to Kinetic Response (Surgical Strikes).
- **2019 (Pulwama/Balakot):** Ending the era of "Strategic Restraint."
- **2019 (August):** The Abrogation of Article 370; structural reset of J&K.
- **2023 (Manipur Crisis):** Realization of "Foreign War-Trainer" influence in ethnic conflicts.
- **2024 (Jammu Pivot):** Mutation of terror tactics from Valley-centric to Hinterland-ambushes.
- **2025 (Operation Sindoor):** First massive use of AI-driven "Ghost Drones" and precision-guided strikes on hybrid cells.
- **2026 (The Sovereign State):** Full operationalization of the PRAHAAR Policy and total digital traceability.

Appendix IV: High-Yield Strategic Data (2025-26)

- **LWE Shrinkage:** Incidents of Naxal violence have dropped by **85%** compared to 2010; the "Red Corridor" is now limited to three core clusters.
- **Border Management: CIBMS (Smart Fence)** is now active across **90%** of sensitive stretches on the Indo-Pak and Indo-Bangla borders.
- **Tourism as Indicator:** Record **21.5 Million tourists** visited J&K in 2025, signaling the defeat of the "Fear Narrative."
- **Cyber Resiliency:** India successfully thwarted over **1.2 Million** state-sponsored cyber-attacks on its power and banking grids in 2025 alone.

Appendix V: Model Questions for Strategic Analysis

1. "The 2026 security matrix suggests that the boundary between Internal and External security has dissolved." Evaluate in the context of the **Two-Front War**.
2. "Digital Radicalization is the 'Open-Source' insurgency of the 21st century." Discuss the effectiveness of the **IT Rules 2025** in maintaining **Cognitive Sovereignty**.
3. Critically examine the impact of **Operation Sindoor** in neutralizing the **Hybrid Terrorist** threat in the Jammu region.
4. "Economic stability is the first casualty of Money Laundering." How do the **PMLA** and **ED** act as guardians of the Indian Republic?

Bibliography

To build the mind of a 2026 strategist, you must move beyond the "general knowledge" booklets and go straight to the **Primary Intelligence** of the Indian State. If you are citing these sources in your UPSC Mains or interviews, you are signaling to the board that you are already thinking like a servant of the Republic.

Here is the authoritative bibliography for **The Sovereign Fortress**.

I. Official Government Reports & Strategic Documents

- **Ministry of Home Affairs (MHA), Annual Report (2024-25 & 2025-26):** The definitive record of the "Zero Tolerance" policy. Focus on the chapters regarding "Internal Security" and "Border Management" for the latest data on the shrinking Red Corridor.
- **NIA Year-End Press Release (Dec 31, 2025):** Specifically for the case studies on the **Pahalgam & Delhi terror probes** and the record **92% conviction rate**.
- **Directorate of Enforcement (ED), Performance Review (March 2026):** Citing the attachment of over **₹32,500 crore** in assets and the **94% conviction rate** under the PMLA, as commended by the FATF.
- **National Security Strategy (NSS) 2025:** The "Proactive Blueprint" that outlines India's shift toward asymmetric capabilities and "Cognitive Sovereignty."

II. The Legislative & Digital Architecture

- **Bharatiya Nyaya Sanhita (BNS), 2023:** * **Section 111:** For the new, rigorous definition of "Organized Crime."
- **Section 113:** For the clinical definition of a "Terrorist Act."
- **Digital Personal Data Protection (DPDP) Rules, 2025:** Notified on Nov 14, 2025. This is essential for understanding the "SARAL" (Simple, Accessible, Rational, Actionable) approach to India's data defense.
- **IT Rules 2025 (Traceability Clause):** The legal mechanism used to puncture the "Digital Safe-Houses" of encrypted radicalization.

III. Institutional Intelligence & Tech Portals

- **I4C (Indian Cybercrime Coordination Centre):** Refer to the **Cyber Multi-Agency Centre (CyMAC)** updates for real-time data on the neutralization of malicious domains and "Cyber-Slavery" syndicates.
- **NATGRID & MAC (Multi-Agency Centre) Briefs:** For understanding the "Whole-of-Government" integration of 11 central agencies to end departmental silos.
- **National Forensic Sciences University (NFSU) Infrastructure Plan 2026:** On the establishment of 9 new campuses to bring "Scientific Justice" to the local police level.

IV. Strategic Analysis & Think Tank "Brain Trust"

- **Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA):**
- *Special Brief (2025):* "From Red Corridor to Naxal-Free Bharat: The Final Push."
- *Strategic Review:* "The Southern Pir Panjal: Analyzing the Jammu Pivot."
- **Observer Research Foundation (ORF):** * *Cyber-Security Series (2026):* "The Sovereign Byte: Navigating the 5th Domain of Warfare."
- *Tech-Policy Paper:* "Deepfakes and the Digital Mob: A National Security Challenge."
- **Vivekananda International Foundation (VIF):** * *Neighborhood Brief:* "ISI's Grey Zone Tactics: Post-Abrogation Realities in J&K."

V. Landmark Doctrines

- **The Sindoor Doctrine (2025-26):** The unofficial but practiced policy of "Disproportionate Retaliation" against terror launchpads and their host state.
- **The PRAHAAR Policy (2026):** The comprehensive 5-point strategy: **P**revention, **R**esponse, **A**ggregation of Capacities, **H**uman Rights, and **A**ttenuating Conditions.

Teacher's Note for the Aspirant:

When writing your answers, don't just list these names. Use them as **Evidence Pillars**. Instead of saying "Cybercrime is rising," say: *"According to the I4C Threat Intelligence Report (2025), India successfully neutralized 1.2 million state-sponsored digital probes, necessitating the full enforcement of the IT Rules 2025 Traceability Clause."* This is the language of a topper.