VISIONIAS
INSPIRING INNOVATION

INTERNAL SECURITY

VALUE ADDED MATERIAL

MAINS 2025

Key Features:

Complete Syllabus Coverage:
Coverage of all key internal security topics, from terrorism to cybersecurity.

Coverage of Emerging Challenges:
Focus on the latest internal security challenges like cyber-attacks, drone warfare, and narco-terrorism.

PYQ-Based Themes:
Incorporates key topics derived from the last 10 years of previous year questions (PYQs).

Efficient Revision Tools:
Use smart tables and infographics for quick revision and better retention.

AHMEDABAD BENGALURU BHOPAL CHANDIGARH DELHI GUWAHATI HYDERABAD JAIPUR JODHPUR LUCKNOW PRAYAGRAJ PUNE RANCHI

INTERNAL SECURITY

Student Notes:

Contents

Preface 4
UNIT 1: LINKAGES BETWEEN DEVELOPMENT AND SPREAD OF EXTREMISM 5
1. Extremism in India: An Overview 5
1.1. Left-Wing Extremism (Naxalism) 6
1.1.1. The Core Nexus: Determinants of Left-Wing Extremism 8
1.2. Government of India's Multi-Layered Counter-Strategy for LWE 10
1.1.1. Security-Based Interventions: Role of Security Forces 10
1.1.2. Development-Based Interventions: Role of Civil Administration 11
1.1.3. Perception Management and Political Engagement 12
1.3. Current Status and Geographical Spread of LWE 12
1.3.1. LWE as a "Violent Internal Security Threat" in current time 13
1.4. Emerging Issues and Challenges 13
1.5. Corrective Strategies and the Way Forward 14
2. North-East Insurgency 15
2.1. Root Causes of Insurgency 16
2.2. State-wise Overview of Insurgency 16
2.3. Approach to Handling Insurgency in NE 19
3. Jammu and Kashmir Insurgency 21
3.1. Root Causes of Insurgency 21
3.2. Approach to Handling Insurgency 22
UNIT 2: ROLE OF EXTERNAL STATE AND NON-STATE ACTORS IN CREATING CHALLENGES TO INTERNAL SECURITY 24
1. External Threats to India's Internal Security 24
1.1. State Actors and Violent Non-State Actors (VNSAs) 25
2. Challenges from External State Actors 26
2.1. Pakistan: The Epicenter of State-Sponsored Terrorism 26
2.2. China: An Ongoing Strategic Threat 27
2.3. Spillover Challenges from Other Neighbours 29
3. Challenges from Non-State Actors 30
3.1. Terrorism 31
3.1.1. The Challenge of Defining “Terrorism” 31
3.1.2. Classifying Terrorist Threats in the Indian Context 32
3.1.3. India's Two-Front War on Terror 32
3.1.4. The Modern Playbook of Terrorism: New Threats and Emerging Challenges 35
3.1.4.1. Hybrid Threats: Technology as a Weapon 35
3.1.4.2. Shifting Battlegrounds: From Borders to Cities and Individuals 38
3.1.4.3. The Invisible Ecosystem of Terror: Over-Ground Workers and Sleeper Cells 39
3.1.4.4. The Blurring Lines: Grey-Zone Warfare 40
3.1.4.5. Evolving Threats: From Military Targets to Civilians in Jammu & Kashmir 40
3.1.4.6. Mobilization of Diaspora for Terrorism 41
3.1.5. India’s Multi-Pronged Counter-Strategy to Terrorism 42
4. Addressing India's Evolving and Interconnected Security Challenges 47
4.1. National Security Strategy: India's Urgent Need 47
UNIT 3: CHALLENGES TO INTERNAL SECURITY THROUGH COMMUNICATION NETWORKS, BASICS OF CYBER SECURITY AND ROLE OF MEDIA AND SOCIAL NETWORKING SITES IN INTERNAL SECURITY CHALLENGES 50
1. Communication Networks and Cyberspace 51
1.1. Criticality of Communication Networks for National Security 52
2. Threats in the Digital Domain: Cyber Warfare, Crime, and Terrorism 53
2.1. State-Sponsored Cyber Warfare and Espionage 54

2.1.1. Cyber Warfare: State-Sponsored Digital Assaults 54
2.1.2. Cyber Espionage: Covert Theft of Sensitive Data 54
2.2. Cybercrime: Attacks for Disruption and Financial Gain 55
2.2.1. Extortion-Based Attacks: Coercion for Profit 55
2.2.2. Theft and Fraud-Based Attacks: Stealing Data and Money 56
2.3. Cyber Terrorism: The Digital Front of Fear 56
3. The Evolving Threat Matrix: The Next Generation of Challenges 57
3.1. The Security Implications of 5G Technology 57
3.2. Artificial Intelligence (AI) as a Dual-Use Technology 57
4. Building Digital Resilience - India's Counter-Strategy 58
4.1. Legal and Policy Framework 59
4.2. Institutional Architecture 59
4.3. Other Key Initiatives and Doctrines 60
4.4. United Nations Convention on Cybercrime 60
5. Role of Media and Social Networking Sites in Internal Security Challenges 63
5.1. Internal Security Threats from Broadcast and Print Media 63
5.2. The Evolving Threat of Social Media to India's Internal Security 65
5.3. Government Measures to Counter Media and Social Media Threats 69
5.3.1. Regulating Traditional and Digital News Media 69
5.3.2. Tackling Threats from Social Media and Online Platforms 69
UNIT 4: MONEY LAUNDERING AND ITS PREVENTION, AND LINKAGES OF ORGANIZED CRIME WITH TERRORISM 71
1. Money Laundering 71
1.1. The Three-Stage Process of Money Laundering 72
1.2. The Evolving Modus Operandi of Money Laundering 72
1.2.1. Traditional Approaches of Money Laundering 73
1.2.2. Modern Approaches of Money Laundering 74
1.3. The Multifaceted Impact of Money Laundering 75
1.4. Key Challenges in Prevention of Money Laundering 77
1.5. The Global Fightback: International Mechanisms for Prevention of Money Laundering . 77
1.5.1. The Financial Action Task Force (FATF) 77
1.5.2. Key International Conventions 78
1.5.3. Other Global Initiatives 78
1.6. India's Legal and Institutional Framework Against Money Laundering 78
1.6.1. Primary Legal Instrument: PMLA, 2002 79
1.6.2. Institutional Mechanisms against Money Laundering 79
1.6.3. Supporting Legal Frameworks 80
1.7. Strengthening Anti-Money Laundering Efforts 81
2. Linkages of Organized Crime with Terrorism 81
2.1. Major Forms of Organized Crime in India 82
2.2. Linkage between Organized Crime and Terrorism 84
2.2.1. The Crime-Terror Nexus 85
2.2.2. Why the Linkage Matters 87
2.2.3. Crime- Terror Nexus in the Indian Context 87
2.2.4. Fighting Organized Crime: Initiatives, Challenges, and the Way Forward 88
UNIT 5: SECURITY CHALLENGES AND THEIR MANAGEMENT IN BORDER AREAS 90
1. Foundations of Border Management 91
2. Key Challenges in Indian Border Management 92
3. Border-by-Border Analysis of Security Challenges 94
3.1. Western Frontier: The India-Pakistan Border 94
3.2. The Northern Frontier: Managing the India-China Border 95
3.3. The Eastern Frontiers - Managing Borders with Bangladesh and Myanmar 96
3.4. Open Borders - Managing Frontiers with Nepal and Bhutan 97

Student Notes:

Student Notes:

3.5. Open Borders - Managing Frontiers with Sri Lanka 98
4. India's Comprehensive Border Management Strategy 99
5. Securing the Maritime Frontiers 102
5.1. Coastal Security Management 103
5.1.2. Indian Coast Guard (ICG) 104
5.1.3. Preventing Maritime Piracy in the Indian Ocean 105
5.1.4. Post-26/11 Initiatives 106
6. Way Ahead: Holistic Approach to Border Management in India 107
UNIT 6: VARIOUS SECURITY FORCES AND AGENCIES AND THEIR MANDATE 108
1. The Multi-layered Nature of India's Security Apparatus 108
1.1. Multi-Layered Security Architecture of India 108
2. National Security Architecture of India 109
3. The Central Intelligence, Investigation and Enforcement Agencies 110
3.1. Intelligence Agencies 110
3.1.1. Intelligence Bureau (IB) 110
3.1.2. Research and Analysis Wing (R&AW) 111
3.1.3. National Technical Research Organisation (NTRO) 111
3.2. Primary Investigative Agencies 112
3.3. Law Enforcement Agencies 114
4. Central Armed Police Forces (CAPFs) 114
4.1. Border Guarding Forces 115
4.1.1. Border Security Force (BSF) 115
4.1.2. Indo-Tibetan Border Police (ITBP) 116
4.1.3. Sashastra Seema Bal (SSB) 117
4.1.4. Assam Rifles (AR) 117
4.2. Internal Security / Anti-Insurgency Forces 118
4.2.1. Central Reserve Police Force (CRPF) 118
4.2.2. Central Industrial Security Force (CISF) 119
4.3. Specialized Security Forces 119
4.3.1. National Security Guard (NSG) 120
5. Role of Armed Forces in Internal Security 121
5.1. Key Joint Military Exercises of India 122
6. State Police Forces and Their Mandate 122
6.1. Structure and Hierarchy 123
6.2. Challenges Faced by State Police 123
6.3. Recommendations for Reform 125
7. Challenges and Reforms in India's Security Apparatus 126
7.1. India’s Integrated Theatre Commands (ITC) 127
7.2. The Changing Face of Combat: Women in Action 128

Preface

Student Notes:

Dear Aspirant,

Congratulations on clearing the Prelims stage of the **Civil Services Examination 2025**. The journey to Mains demands not only a robust knowledge base but also a nuanced understanding of interconnected subjects, especially in a crucial area of **GS Paper 3 like Internal Security.**

We recognize that this critical period can be daunting. With a syllabus including topics that constantly evolve, are associated with complex geopolitical dynamics, and emerging non-traditional threats, you might find yourself grappling with questions like: *How do I cover the vast spectrum of internal security challenges, from Left-Wing Extremism to cyber warfare? How do I effectively analyze current developments in border management, intelligence, and counter-terrorism strategies to write comprehensive answers?*

It is with a deep appreciation for these challenges that we, the team at **VISIONIAS**, have meticulously prepared this **Internal Security Value Added Material (VAM) for Mains 2025**. This document is not merely a compilation; it is a strategic guide designed to empower your preparation for the GS Paper 3.

The Philosophy: Precision and Relevance of Content

The cornerstone of this VAM is a thorough and objective analysis of UPSC Mains questions from recent years. This rigorous PYQ analysis serves as the guiding principle of picking themes and topics to discuss in this document, ensuring that every aspect of the document is aligned with the examination's demands.

How Will This Document Empower Your Mains Preparation?

Our primary objective is to equip you with the comprehensive content and the analytical acumen necessary to excel in UPSC CSE Mains. This VAM is structured to achieve several key objectives:

- **Comprehensive Coverage of Internal Security Dimensions:** We have meticulously covered **all major facets of India's internal security,** including linkages between development and extremism, the role of external state and non-state actors, challenges from communication networks and cyber threats, money laundering, border management, and the mandates of various security forces and agencies.
- **Integrated Strategic Approaches and Policies:** Recognizing the dynamic nature of this subject, **key government strategies**, doctrines (like SAMADHAN), policies (e.g., National Cyber Security Policy), and legal frameworks (e.g., UAPA, PMLA) pertinent to tackling internal security threats are **seamlessly integrated** throughout the document, ensuring your preparation is always up-to-date.
- **Focus on Analytical Insights and Emerging Threats:** This document delves into critical **contemporary issues** such as urban naxalism, the drone threat, grey-zone warfare, and the crime-terror nexus, providing data-driven insights into their evolving nature, challenges, and India's counter-strategies.
- **One-Stop Solution:** This comprehensive document **addresses the entirety of the syllabus,** consolidating all necessary topics into a single, accessible resource, thereby saving your valuable time and effort in navigating multiple sources.

Our Commitment to Your Success

This document is a culmination of dedicated effort aimed at simplifying your preparation and **maximizing your score for Mains 2025**. We firmly believe that with a clear strategy and the right resources, your diligent efforts will translate into commendable success.

Trust this process, utilize this material to its fullest potential, and approach the examination hall with the confidence that you are thoroughly prepared.

Your Trusted Partner in Success Vision IAS

Vision IAS

Student Notes:

UNIT 1: LINKAGES BETWEEN DEVELOPMENT AND SPREAD OF EXTREMISM

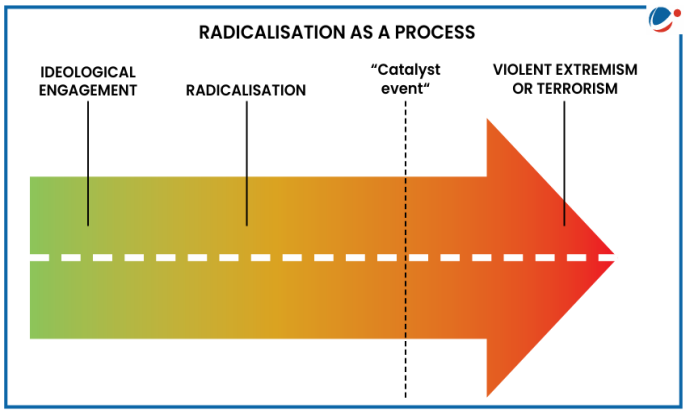
Previous Years Question

- **2022**:**Question**: Naxalism is a **social, economic**, and **developmental issue** manifesting as a **violent internal security threat**. In this context, discuss the **emerging issues** and suggest a **multilayered strategy** to tackle the menace of **Naxalism**.(**Marks**: 10 mark.)
- **2020**:**Question**: What are the **sound determinants** of **left-wing extremism** in the **Eastern part of India**? What **strategy** should the **Government of India**, **civil administration**, and **security forces** adopt to counter the threat in the affected areas?(**Marks**: 15 marks)
- **2018**: **Question**: **Left Wing Extremism (LWE)** is showing a **downward trend**, but still affects many parts of the country. Briefly explain the **Government of India's approach** to counter the challenges posed by **LWE**.(**Marks**: 10 marks)
- **2015**:**Question**: The persisting drives of the **government** for **development** of large industries in **backward areas** have resulted in isolating the **tribal population** and the **farmers** who face multiple **displacements** with **Malkangiri** and **Naxalbari** foci, discuss the **corrective strategies** needed to win the **left wing extremism (LWE)** doctrine-affected citizens back into the mainstream of **social** and **economic growth**.(**Marks**: 15 marks)
- **2013**:**Question**: **Article 244** of the Indian Constitution relates to the **Administration of Scheduled areas** and **tribal areas**. Analyze the impact of **non-implementation** of the provisions of the **fifth schedule** on the growth of **Left Wing Extremism**.(**Marks**: 12.5 marks)

1. Extremism in India: An Overview

Extremism refers to beliefs or actions that are far beyond what society considers normal or acceptable. It is characterized by:

- **Intolerance towards opposing views**
- Advocacy of **radical measures or violence** to achieve **political, social, or religious goals**



In India, extremism is a significant internal security threat, arising from a combination of **historical, political, and social grievances**. The manifestations of extremism in India can be broadly categorized as follows:

Category	Type of Extremism	Description	Key Examples/Details
1. Religious Extremism	**Islamic Extremism**	**Driven by** radical religious ideologies, justifying violence or intolerance.	• Motivated by global jihadi movements and state-sponsored agendas. • Radicalization of youth to join groups like **ISIS** and **Al-Qaeda**. • Goal: Establishment of an Islamic caliphate or inciting communal violence.

2. Ethno-Nationalist Extremism	**Insurgency in Northeast India**	Driven by **ethnic identity** and a **desire for autonomy or secession**.	• Groups like **ULFA** and **NSCN factions are waging** armed struggles. • Rooted in grievances related to **neglect by the mainland**.
	Separatist Movements	Movements advocating for secession or independence from the Indian Union.	• **Kashmir Insurgency**: Fueled by cross-border support. • **Khalistan Movement**: Periodically revived in **Punjab**, often overlapping with religious extremism.
3. Left-Wing Extremism (LWE)	**Naxalism**	Radical **far-left ideology** rooted in communist principles aiming for a classless society through revolution.	• Focuses on **socio-economic inequality** and exploitation of marginalized communities. • Primarily affects **tribal and rural populations** in the **"Red Corridor"** with deep-seated developmental grievances.

Understanding Insurgency vs Terrorism

Attribute	Insurgency	Terrorism
Definition	Organized, protracted armed rebellion against an established authority	Use of violence or threat to instill fear for political ends
Motivation	Political, social, economic, or ethnic grievances; regime change	Political, religious, or ideological objectives
Targets	Primarily government forces, military, infrastructure	Civilians, non-combatants, symbolic targets
Tactics	Guerrilla warfare, sabotage, ambushes, hit-and-run attacks	Bombings, assassinations, hostage-taking, suicide attacks
Goals	Overthrow/challenge government, control territory, autonomy	Instill fear, provoke overreaction, force political change
Organization	Often hierarchical, with command and control	Often decentralized, cell-based, secretive

1.1. Left-Wing Extremism (Naxalism)

"Political power grows out of the barrel of a gun." - Mao Zedong.

This famous quote directly **encapsulates the Maoist philosophy of violent struggle for political power**, central to LWE ideology. **LWE** or **Naxalism** refers to the use of **violence** by various **communist guerrilla groups** to destabilize and ultimately overthrow the **democratically elected state**.

- It is a form of **insurgency** that seeks to capture **state power** through violent armed struggle.

- The **Union Government** has categorized the **Communist Party of India (Maoist)**, or **CPI (Maoist)**, and all its front organizations as a '**terrorist organization**' under the **Unlawful Activities (Prevention) Act** (**UAPA**).

Marxism-Leninism-Maoism forms the ideological **foundation** of **Left-Wing Extremism (LWE)** in India. The **Naxalites** see India as a semi-feudal, semi-colonial state controlled by a wealthy class. They follow **Mao Zedong's** idea that **"political power grows out of the barrel of a gun"**, rejecting democracy and aiming for a **New Democratic Revolution** through a **'Protracted People's War'**, a military strategy. This involves:

1. **Armed insurgency** by guerrilla armies.
2. **Mass mobilization** of marginalized groups, particularly Adivasis and poor peasants.
3. **Building alliances** with sympathetic groups to strengthen their cause.

Maoist Paradox: Beliefs vs. Battleground

Maoists reject tribal beliefs like worshipping **'Dharti Mata'** as superstitions. However, they use tribals' strong connection to the land and their spiritual beliefs to rally against mining projects.

For example, the **Dongria Kondh** tribe in **Niyamgiri** worships **"Niyam Raja"** as the protector of their land. Maoists have opposed these rituals, calling them **"anti-revolutionary superstition"**, creating a divide among the tribals.

This shows a key contradiction in Maoist ideology. While they **oppose tribal beliefs** based on their atheist views, they use these cultural grievances to push their own agenda.

Global Parallel: Peru's Shining Path

Peru's **Shining Path** utilized **Maoist ideology** to recruit **indigenous communities**. However, their **extreme violence against civilians** led to significant **backlash** from the very population they aimed to liberate.

This case highlights how **ideological rigidity** combined with ruthless methods ultimately **alienates local populations**, undermining insurgent movements despite initial appeals.

Historical Evolution of LWE in India

The Naxalbari Uprising (1967) and its Legacy

- The origins of Naxalism lie in the **Naxalbari Uprising (1967)** in West Bengal, led by **Charu Majumdar**, **Kanu Sanyal**, and **Jangal Santhal**. It was a response to the **exploitation of peasants by landlords a**nd the failure of land reforms.
- Though the uprising was suppressed, it sparked similar movements across India, giving rise to the term "Naxalism."

Post-Rebellion Pathway: Philippines

The **Philippines' Hukbalahap Rebellion settlement** is a key **best practice** in **post-rebellion reconciliation**. It successfully **integrated former rebels** into society, primarily through impactful **land reforms**.

This example highlights the critical importance of **addressing core grievances** and **offering socio-economic pathways** to disarmed combatants for lasting peace and stability.

Phases of Consolidation, Expansion, and Decline

- **Initial Phase (1967-1980)**: The movement spread but was largely crushed by the state by the mid-1970s.
- **Resurgence and Consolidation (1980-2004)**: The People's War Group (PWG) in Andhra Pradesh and Maoist Communist Centre of India (MCCI) in Bihar grew as the most powerful outfits.
- **Peak Expansion (2004-2010)**: The merger of PWG and MCCI formed the **CPI (Maoist)** in 2004, leading to a significant escalation in violence and territorial expansion, particularly the "Red Corridor."
- **Decline (2011-Present)**: Government strategies combining security actions and development initiatives have led to a decline in LWE violence and influence.

Student Notes:

Student Notes:

1.1.1. The Core Nexus: Determinants of Left-Wing Extremism

Left-Wing Extremism (LWE) is **influenced by socio-economic, developmental,** and **governance failures.** It is not just a law-and-order challenge but a deep-rooted problem that thrives on grievances exploited by extremist groups. **Key determinants of LWE include:**

Development-Extremism Vicious Cycle

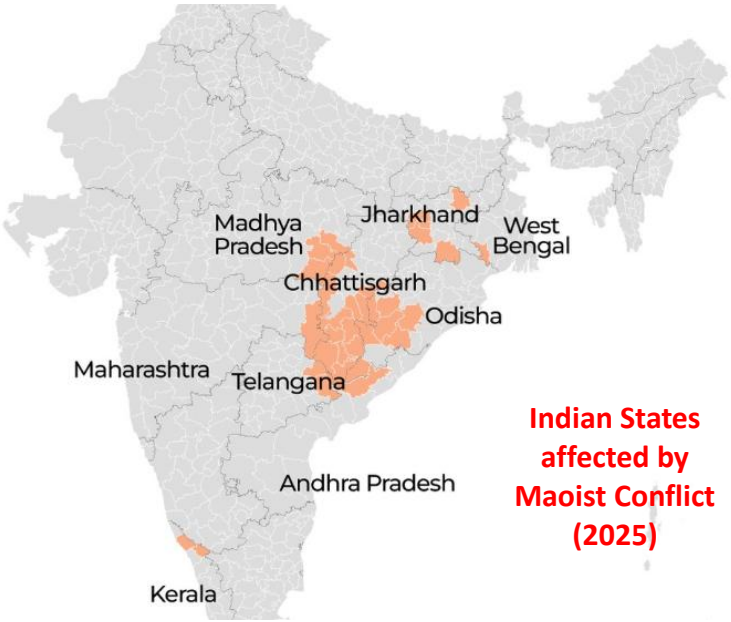
The link between underdevelopment and extremism is cyclical:

- **Underdevelopment** fuels extremism, and
- **Extremism** further impedes development, creating a self-perpetuating trap.

How Underdevelopment Creates Fertile Ground for Extremism	How Extremism Impedes Development
Severe Infrastructure Deficits: Lack of **roads**, **electricity**, **water**, and **healthcare** fuels frustration, making people vulnerable to extremism	**Destruction of Infrastructure**: Naxalites destroy infrastructure such as schools, roads, and communication towers to isolate the population and disrupt governance.
High Poverty and Unemployment: **Limited jobs** and high **poverty** create fertile ground for Naxal recruitment	**Deterrence of Investment**: Extremist activities create a high-risk environment, deterring investment and halting critical development projects.
Low Human Development Indicators: **Low education**, **poor healthcare**, and **social deprivation** fuel frustration, aiding extremist ideologies.	**Cycle of Underdevelopment**: Extremism blocks development, maintaining the cycle of poverty and underdevelopment in the region.

Developmental and Economic Determinants

The **conflict over resources**, particularly land and water, is central to LWE in tribal regions, often summed up by the slogan **"Jal, Jangal, Jameen"** (Water, Forest, Land).



1. **Land Alienation and Forced Displacement**
   - **Flawed development model**: Large projects like dams and mining have displaced tribal communities.
   - **Mass displacement**: Tribals have been displaced without proper compensation or rehabilitation, leading to their status as **"ecological refugees."**

Student Notes:

2. **Impact of Large Industries and Mining Projects on Tribal Populations**
   - **State-corporate nexus**: State policies often enable the acquisition of tribal land for corporate use, ignoring exposure to **pollution** and **unsafe working conditions**.
   - **Loss of traditional rights**: Mining and industrialization destroy tribal economies and deny them access to forest resources.
3. **The "Resource Curse"**
   - **Unequal distribution of benefits**: Although rich in minerals like coal and iron ore, these regions rarely benefit from the profits. Instead, they face **environmental damage** and loss of livelihood.
4. **Lack of Livelihood Opportunities and Food Insecurity**
   - Destruction of traditional economies, without alternatives, has led to **chronic unemployment** and **food insecurity**, pushing people towards extremism.

Global Parallel: Lessons from Colombia's "Resource Curse"

Colombia has actively managed its **"Resource Curse"** by implementing **royalty-sharing** with communities in **mining zones**.

This aims to distribute wealth more equitably, fostering local development & to counter armed groups.

Governance and Administrative Deficits

The state's failure to protect its citizens and deliver services creates a void that Naxalites have exploited.

1. **Failure to Implement Constitutional Safeguards**
   - **Article 244** and the **Fifth Schedule** grant **autonomy** to **Scheduled Areas** to protect **tribal land** and **culture**, but the **state** has been ineffective in ensuring protection..
2. **Poor Implementation of Protective Legislations**
   - **PESA Act, 1996**: Intended to grant **Gram Sabhas** the right to self-governance, but its provisions have been violated.
   - **Forest Rights Act (FRA), 2006**: Meant to restore the rights of forest-dwelling communities, but poor implementation has left many communities disenfranchised.
3. **Administrative Vacuum, Corruption, and Ineffective Grievance Redressal**
   - In many LWE-affected areas, **state presence** is minimal, and Naxalites have established a parallel government (Janatana Sarkar), administering justice through **Jan Adalats** and collecting "taxes."

Indigenous Empowerment: Canada's Model

Canada's Indigenous Self-Government Agreements serve as a global **Tribal Governance Model**. These agreements explicitly grant **land and resource rights** to **Indigenous communities**, recognizing their inherent autonomy.

This approach aims to directly reduce the historical **alienation**, **fostering self-determination** and improving socio-economic outcomes through self-governance.

Social and Political Determinants

In addition to economic and governance issues, deep-seated social injustices contribute to the persistence of LWE.

1. **Social Exclusion, Oppression, and Erosion of Tribal Dignity**

   Tribal communities have long faced:

   - **Cultural oppression** and humiliation.
   - Their unique languages, cultures, and traditions are often viewed as "**backward**," leading to a loss of dignity and a sense of alienation.
2. **Lack of Political Mobilization and Voice for Tribal Communities:** Despite **reservations** in legislatures, the political voice of tribal communities remains weak, with tribal leaders often co-opted, leaving extremism as the only viable alternative.

Student Notes:

3. **Human Rights Violations and Mistrust in Security Forces:** The **heavy-handed approach** by security forces, including fake encounters and illegal detentions, has created deep **mistrust** between the local population and the state's security apparatus.

1.2. Government of India's Multi-Layered Counter-Strategy for LWE

The Government of India previously focused on LWE as a pure security concern. However, it has shifted from a purely security-centric approach to a more holistic and multi-layered strategy to counter Left-Wing Extremism. This approach tackles the problem on multiple fronts: **security**, **development**, and **perception**.

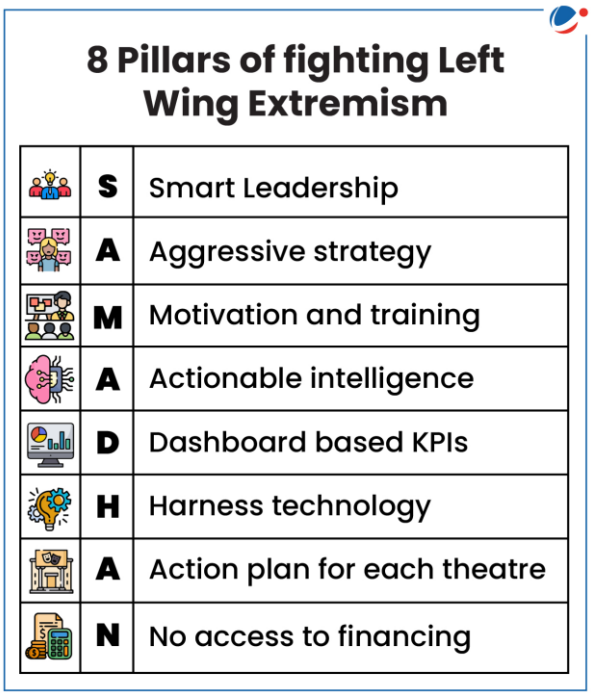
The National Policy and Action Plan (2015)

The cornerstone of the government's new approach is the **National Policy and Action Plan**, introduced in 2015. The policy **treats LWE as a shared responsibility between the Centre and the States** and is based on a two-pronged strategy:

1. **Security Interventions**: These aim to create a secure environment that allows development to take place.
2. **Development and Rights**: Focuses on addressing the root causes of the conflict by ensuring the rights and entitlements of local populations and accelerating development.

The SAMADHAN Doctrine

In 2017, the government introduced the **SAMADHAN Doctrine**, a holistic **framework for security operations.** This doctrine emphasizes **proactive, intelligence-driven operations** supported by **technology**.



1.1.1. Security-Based Interventions: Role of Security Forces

The security aspect of the strategy focuses on reducing violence and curbing the influence of Naxalites.

1. **Operations by Central Armed Police Forces (CAPFs) and State Police**

   A robust security framework has been established in affected areas:

   - **COBRA Battalions**: Specially trained Commando Battalions for Resolute Action (COBRA) have been deployed for jungle warfare and targeted operations.
   - **State-Level Forces**: Specialized forces like the **Greyhounds** in Andhra Pradesh and Telangana, and the **Black Panthers** in Chhattisgarh, have proven highly effective.
   - **Bastariya Battalion**: The CRPF has created a unique initiative by recruiting local tribal youth from Bastar into a specialized **Bastariya Battalion**, leveraging their local knowledge and language skills.

2. **Strengthening Intelligence Networks and Inter-State Coordination**

   Intelligence is central to counter-LWE operations.

   - Strengthening state intelligence bureaus and improving coordination through platforms like the **Multi-Agency Centre (MAC)** ensures better collaboration between states.
   - **Joint task forces** help prevent extremists from exploiting administrative boundaries.

Student Notes:

1.1.2. Development-Based Interventions: Role of Civil Administration

The civil administration plays a critical role in breaking the Naxalite narrative of state apathy.

1. **Infrastructure Development: Road Requirement Plan (RRP) and Mobile Tower Projects**

   To counter **developmental deficit**, significant efforts are being made to enhance infrastructure:

   - **Road Connectivity**: The **Road Requirement Plan (RRP)** focuses on improving road access in remote areas, aiding both security forces and economic activity.
   - **Digital Connectivity**: A mobile tower project is underway to improve communication, administration, and public service delivery.

2. **Socio-Economic Development Schemes: Education, Health, and Skilling**

   Targeted socio-economic initiatives are being implemented for marginalized communities:

   - **Education**: New schools, including **Eklavya Model Residential Schools** and **Kendriya Vidyalayas**, are being established to offer quality education to tribal children.
   - **Skilling and Livelihoods**: The **Roshni scheme** is a placement-linked skill development program aimed at rural youth from LWE-affected districts.

3. **Financial Inclusion and Public Service Delivery**

   To extend the formal economy and state services:

   - New **bank branches**, **post offices**, and **ATMs** are being opened to promote financial inclusion.
   - The **Direct Benefit Transfer (DBT)** system is being used to ensure the delivery of welfare schemes.

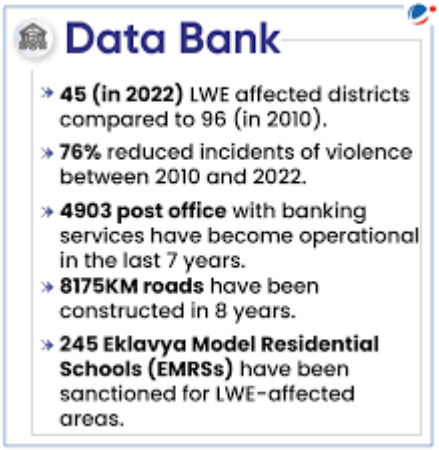
4. **Aspirational Districts Programme**

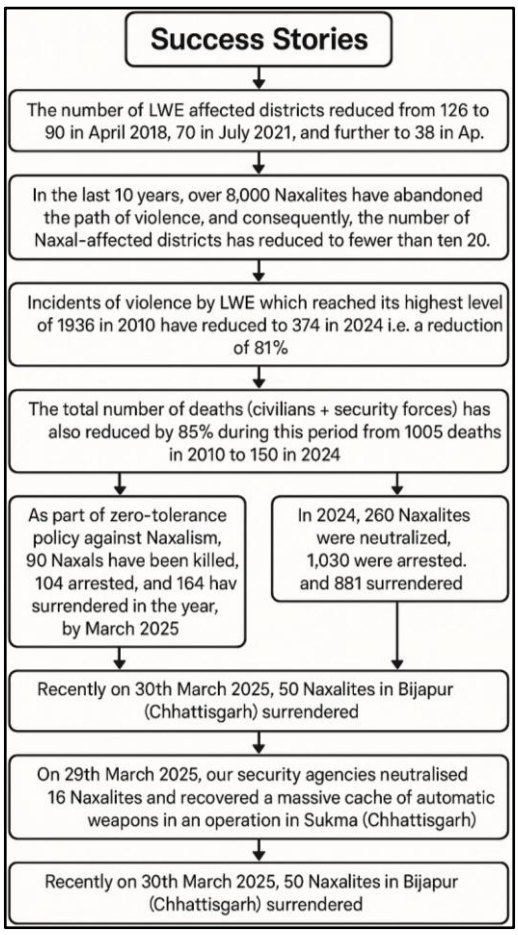
   A **significant number of LWE-affected districts** are also part of the **Aspirational Districts Programme**. This data-driven initiative focuses on improving socio-economic indicators through coordinated efforts by the central and state governments.

Community-Driven Development (CDD) in the Philippines: Empowering Locals

The **Kalahi-CIDSS** program in the **Philippines** empowers **communities** in conflict zones to implement **small-scale development projects**, fostering **ownership** and **self-reliance**.

A **World Bank** study found that a 10% increase in **CDD funding** led to a **3.5% decrease** in violent incidents, **countering insurgent narratives** of state neglect and promoting **peacebuilding**.





Student Notes:

1.1.3. Perception Management and Political Engagement

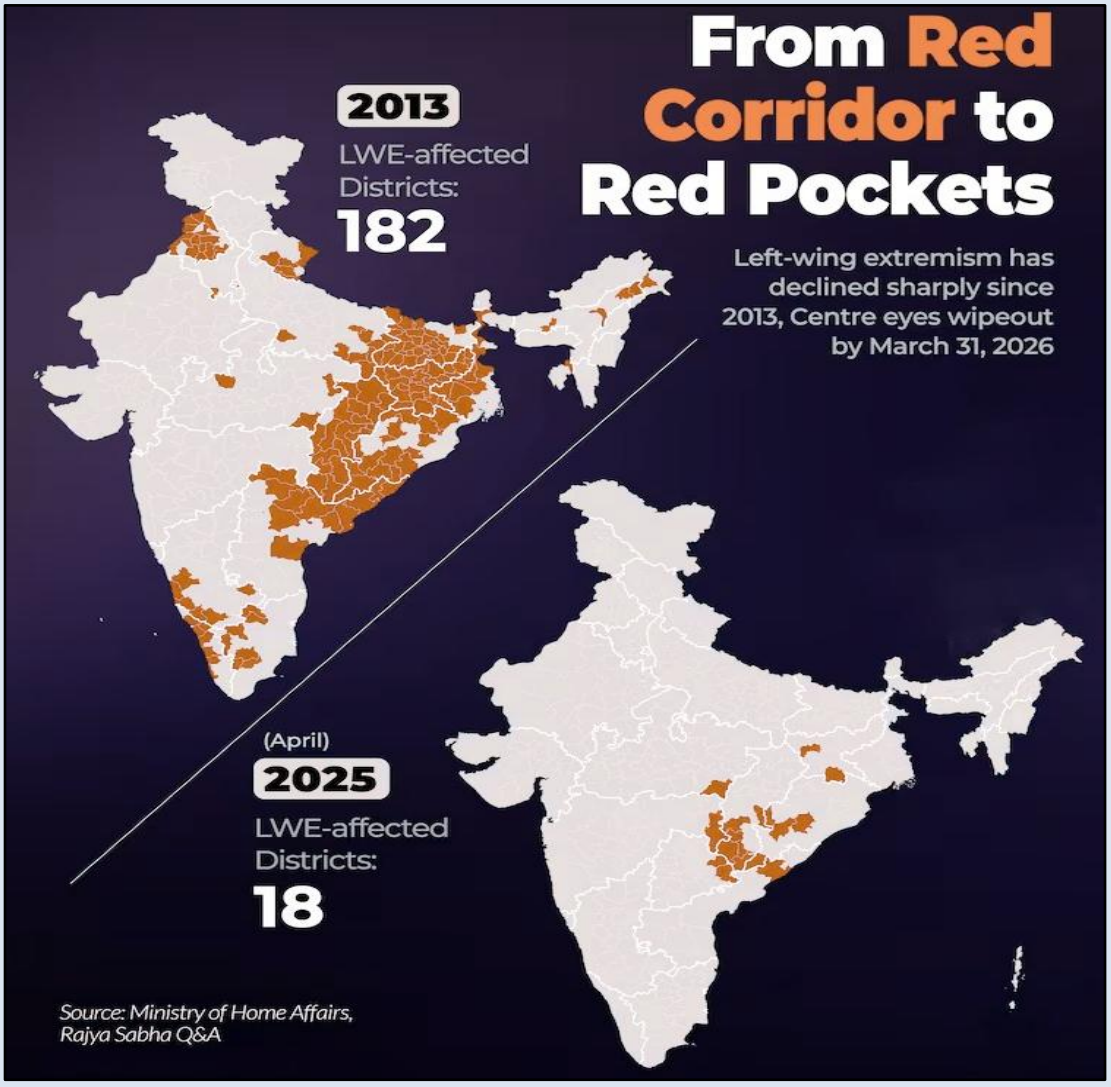
1. **"Winning Hearts and Minds" (WHAM) Approach**
   The government employs **Civic Action Programmes** where security forces engage with the local community.
   - These programs offer medical assistance, distribute essential goods, and organize sports events to bridge the trust deficit between the people and the state.
2. **Surrender and Rehabilitation Policies**
   - States have implemented **Surrender and Rehabilitation Policies** to encourage Naxalites to renounce violence and reintegrate into mainstream society.
   - These policies offer financial assistance, vocational training, and other incentives to weaken the extremist ranks.

1.3. Current Status and Geographical Spread of LWE

Contraction of the "Red Corridor": 90% of all LWE violence is now concentrated in just **18 districts**, with states like **Chhattisgarh**, **Jharkhand**, and **Odisha** remaining the epicenters.

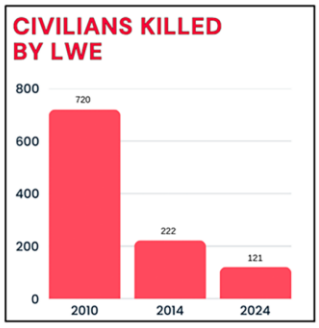
Government of India to End Left-Wing Extremism (LWE) by 2026

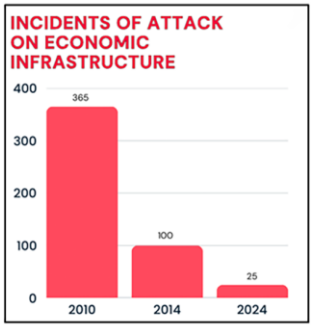
The **Government of India's approach** aims to **completely eliminate LWE** by **2026** through enhanced **security**, **development**, and **rehabilitation** efforts, marking the final phase of the LWE fight. The approach includes a **zero-tolerance policy**, strong **Centre-State cooperation**, and public participation to eliminate extremist support.



Student Notes:

1.3.1. LWE as a "Violent Internal Security Threat" in current time





- Despite the decline, LWE continues to be a significant internal security challenge.
- **Official Designation**: Former Prime Minister **Manmohan Singh** described LWE as the "single biggest internal security threat" to India.
- **Deadliest Outfit**: **CPI (Maoist)**, identified by the **Global Terrorism Index (GTI)** as the deadliest terrorist group in India, remains responsible for significant terror-related attacks and deaths, threatening national security.

1.4. Emerging Issues and Challenges

Despite significant successes in containing Left-Wing Extremism (LWE), the movement continues to evolve, presenting new challenges that require adaptive and corrective strategies. These challenges reflect changes in tactics, funding, and operations that need urgent attention.

1. **"Urban Naxals" and Frontal Organizations**

   As their influence diminishes in rural areas, Naxalites have increasingly focused on building networks in urban settings. This shift is marked by:

   - **"Urban Naxals"**: The term, although not defined officially by the Government of India, refers to intellectuals, activists, and students in urban areas who are seen as providing ideological justification, legal aid, and logistical support for the LWE movement. These individuals often serve as the **propaganda machinery**, creating a sympathetic narrative for the extremists.
   - **Frontal Organizations**: These are **seemingly legitimate civil society groups** used by Naxalites to raise funds, spread Maoist ideology, and mobilize support. They **operate in the grey zone,** blurring the lines between activism and extremism.

2. **Diversification of Funding: From Extortion to Linkages with Organized Crime**

   Naxalites have diversified their financial streams, moving beyond traditional extortion to engage in more sophisticated operations:

   - **Extortion Economy**: They continue to collect "taxes" from contractors, businesses, and corrupt officials in affected areas.
   - **Linkages with Organized Crime**: Growing evidence suggests connections with criminal syndicates involved in **drug trafficking**, **illegal mining**, and other illicit activities, which help fund their operations.

3. **Use of Technology for Propaganda and Improvised Explosive Devices (IEDs)**

   Naxalites have increasingly used technology to further their cause:

   - **Propaganda**: Social media and digital platforms have become essential tools for spreading propaganda and recruiting youth to their cause.
   - **IEDs**: The use of Improvised Explosive Devices (IEDs) remains a critical challenge, with these weapons being responsible for a significant number of casualties among security forces. The growing sophistication of IEDs has made countermeasures more difficult.

Student Notes:

4. **The Challenge of Preventing the Re-emergence of LWE in Cleared Areas**

   Once an area is cleared of Naxalite influence, the **administrative and developmental vacuum** must be filled swiftly to prevent the resurgence of extremism. The failure to establish effective governance and development in cleared areas creates a risk for the Naxalites to regroup and regain control.

1.5. Corrective Strategies and the Way Forward

To address the evolving challenges of Left-Wing Extremism, several corrective strategies need to be implemented:

1. **Ensuring Effective Implementation of Protective Laws (FRA, PESA)**

   A key corrective strategy is the **effective implementation** of protective laws such as the **Forest Rights Act (FRA)** and the **PESA Act**. This includes:

   - Recognizing **community forest rights**.
   - Empowering **Gram Sabhas** to take control over local resources.
   - Ensuring that the intended benefits of these laws reach the local populations, thus addressing some of the root causes of the conflict.

2. **Adopting a More People-Centric and Participatory Development Model**

   The development model should be more **inclusive and participatory**:

   - Local communities must be **active stakeholders** in planning and implementing development projects.
   - A shift away from top-down approaches to more grassroots-driven initiatives can help empower local populations and reduce discontent.

3. **Strengthening Local Self-Governance and Empowering Gram Sabhas**

   Empowering **local democratic institutions** is crucial:

   - Granting true **administrative and financial autonomy** to **Gram Sabhas** as envisioned in the PESA Act is essential.
   - This empowerment fosters a sense of ownership and counters the Naxalite narrative of an exploitative state, thus addressing key socio-political grievances.

4. **Police Reforms and Sensitization of Security Forces**

   To build trust, there is a need for continuous **sensitization of security forces**:

   - Security personnel must be trained in **human rights** and the local culture of tribal populations.
   - Police forces should be viewed as **service providers and protectors**, rather than merely instruments of state coercion. This would help in building stronger relationships between the local population and the authorities.

Insights from Recommendations of Key Committees

D. Bandyopadhyay Committee: This committee highlighted that the state had **abdicated its responsibility** in affected areas. It recommended a **tribal-friendly land acquisition** and **rehabilitation policy**, which should be adopted to address longstanding grievances and ensure a lasting solution to the LWE problem.

Model of Success for LWE: Case Study

Model	Key Features	Approach
Andhra Pradesh "Greyhounds" Model	**Elite Commando Force**: Specially trained forces in jungle warfare and guerrilla tactics.	Security-driven, targeting Maoist strongholds with high mobility and precision.

Student Notes:

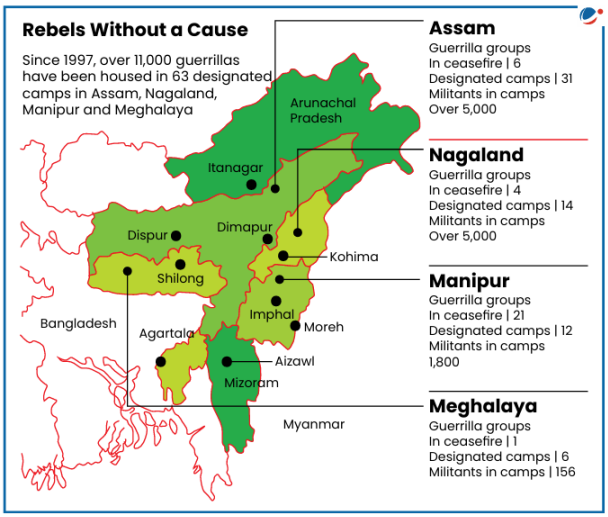
	Local Intelligence Network: Grassroots intelligence network for targeted operations.	Intelligence-driven operations to engage Maoist squads.
	Small Team Operations: Small, well-equipped teams with high mobility.	Small teams enable quick engagement with Maoist hideouts.
	Leadership and Political Will: Strong backing from state leadership ensuring resources and autonomy.	Political support was key for operational success and autonomy.
	Effective Surrender Policy: Encouraged Naxal cadres to surrender and reintegrate into society.	Complementary surrender policy for reducing the movement's manpower.
Saranda Development Plan (Jharkhand)	**Clear-Hold-Build Strategy**: Three-phase strategy: Clear (military operation), Hold (establish security), Build (development).	Integrated security and development model with a focus on reclaiming and developing areas.
	Saturation of Development: Development of infrastructure such as roads, schools, and welfare schemes.	Post-security stabilization with large-scale infrastructure development.
	Winning Trust: Focus on tangible benefits for local communities to counter Maoist propaganda.	Building trust with the tribal population by showing state benefits.

Student Notes:

2. North-East Insurgency

The North-Eastern region of India, comprising the 'Seven Sister' states, has historically been a hotbed of insurgent activities.

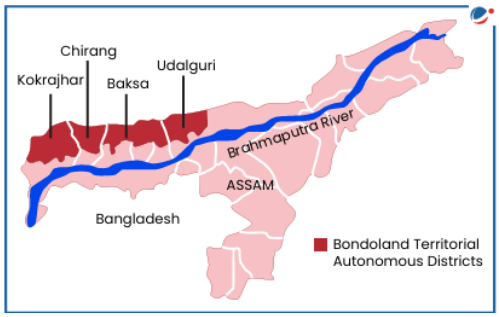
2.1. Root Causes of Insurgency



1. **Historical Alienation and Identity Issues**: After independence, regions inhabited by **Tibeto-Burman/Mongoloid** ethnic groups felt disconnected from the newly formed Indian nation-state. The colonial **frontier area** approach led to a lack of central governance, fostering a distinct identity and ethnic conflicts.
2. **Immigration and Demographic Shifts**: Influxes of **immigrants**, especially from **Bangladesh**, have caused anxiety among indigenous populations about preserving their **cultural identity** and control over resources, fueling **nativist sentiments** and conflicts.
3. **Economic Underdevelopment and Negligence**: Despite rich **natural resources**, the region faces **economic underdevelopment**, high **unemployment**, and poor **infrastructure**. The perception of **central government negligence** and corruption has created frustration, which insurgent groups exploit for recruitment.
4. **Geographical Terrain and External Support**: The **rugged terrain** along borders with **Myanmar**, **Bangladesh**, and **Bhutan** provides safe havens for insurgents. Support from neighboring countries and criminal groups, like the **Golden Triangle's drug trade**, has helped sustain these insurgencies.
5. **Political Motivations and Demands**: Insurgents gain popular support by articulating political causes, such as demands for **sovereignty** (e.g., **Greater Nagalim** by **NSCN-IM**) or separate states based on **ethnic identity** (e.g., **Bodoland** by **NDFB**, **Kuki homeland** by **UKLF**).

2.2. State-wise Overview of Insurgency

Assam:



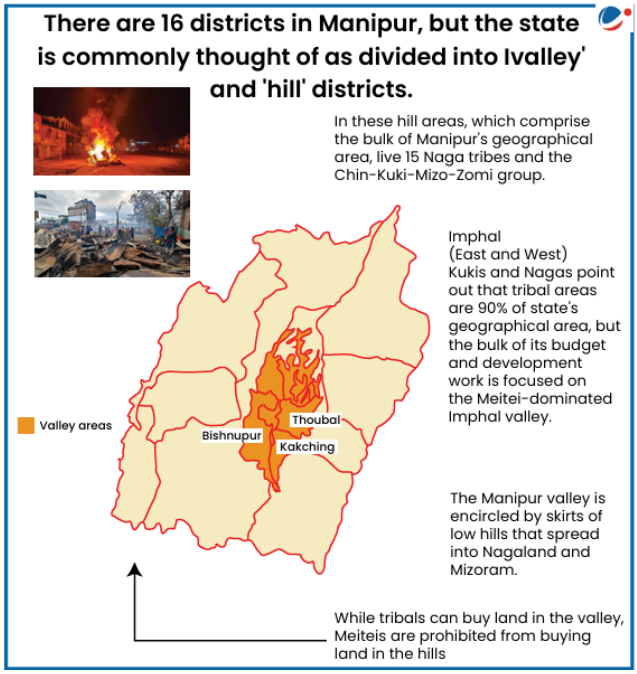
- **Key Issues:**
  - Assam has historically faced **insurgency** from groups like the **United Liberation Front of Assam (ULFA), National Democratic Front of Bodoland (NDFB), and Kamtapur Liberation Organization (KLO).**
  - These groups often articulate demands for **sovereignty or separate homelands** based on ethnic identity.
  - The state also grapples with issues of **illegal immigration**, leading to demographic shifts and the contentious **National Register of Citizens (NRC)** process.
  - **Inter-state border disputes** with neighboring North-Eastern states have also been a persistent challenge.
- **Approach:**
  - The government has pursued a **multi-pronged strategy. Peace accords,** such as the Bodo Peace Accord (2020) with various Bodo groups, have aimed to resolve long-standing

Student Notes:

demands for a separate Bodoland, resulting in increased autonomy for the Bodoland Territorial Region (BTR).
- Other agreements, including the **Adivasi Peace Accord (2022) and Karbi Anglong Agreement (2021),** address grievances of other ethnic communities.
- **Boundary agreements** with Arunachal Pradesh (2023) and Meghalaya (2022) are resolving inter-state border disputes.
- The **NRC update** was a significant, albeit controversial, measure to identify illegal immigrants.

Manipur:

- **Key Issues:**
  - Manipur experiences **insurgency** from numerous valley-based groups like the **People's Liberation Army (PLA), United National Liberation Front (UNLF), and various factions of PREPAK, KCP, KYKL, MPLF, and RPF.**
  - The state has recently witnessed **significant ethnic violence,** particularly the conflict between the **Meitei community** (residing primarily in the valley) and **Kuki-Zomi tribes** (inhabiting the hills).
  - This conflict is fueled by complex issues including **land rights, demographic changes, demands for Scheduled Tribe** status for the Meiteis, and concerns over illegal settlements, exacerbated by refugees from Myanmar.



- **Approach:**
  - The government has engaged in peace agreements, such as with the UNLF, to **bring insurgent groups** into the **mainstream**.
  - Long-term measures include strengthening border management to **prevent illegal entry,** promoting **development** in **remote hill areas,** and carefully **deliberating the Meitei community's demand** for ST status, considering recommendations from various expert committees.

The Manipur Ethnic Violence Crisis: A Brief Overview

On **May 3, 2023**, large-scale ethnic violence broke out in **Manipur** between the **Meitei community** (Hindu, majority, in Imphal valley) and the **Kuki-Zo tribal community** (Christian, in the hills). Over **260 killed**, **60,000 displaced**, thousands of homes destroyed, and many people are still living in relief camps.

- The violence was triggered by a protest against the **Manipur High**

Student Notes:

Court's order recommending **Scheduled Tribe (ST)** status for the Meitei community.

- This would grant the Meiteis access to **reserved jobs** and **land rights**, which the Kuki-Zo feared would diminish their own protections.

Factors That Escalated the Violence

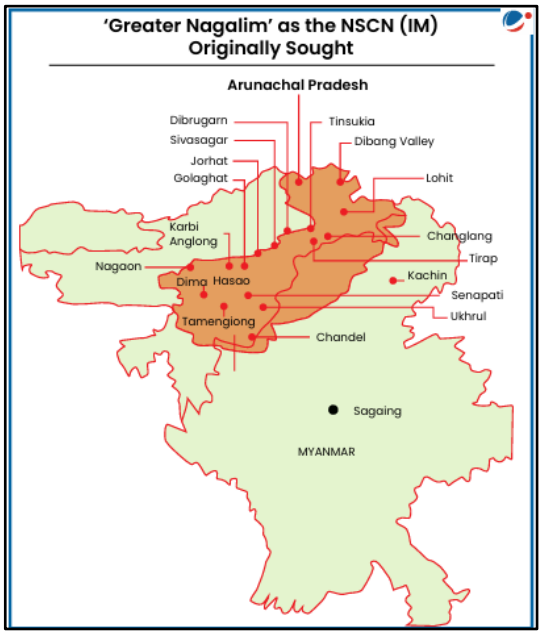
- **Ethnic Tensions**: Long-standing disputes over **land**, **jobs**, and **political power** between the Meitei and Kuki-Zo communities.
- **Historical Grievances**: Tribal groups felt marginalized by government policies and demographic shifts.
- **Other Factors**: **Armed groups, drug trafficking** routes from **Myanmar**, and **looted weapons** contributed to escalating violence.

Government Response

- Curfews and **internet shutdowns** were imposed.
- Thousands of **security personnel** deployed, and **"shoot at sight" orders** issued to control the violence.
- Additional security forces were sent, and a **peace committee** was set up, though it failed due to lack of trust.
- **President's Rule** was imposed in **February 2025** after the **Chief Minister's resignation** which still continues till date.

Despite interventions, **peace has not been achieved**, and the state remains divided along ethnic lines. Displaced families still face uncertainty.

Nagaland:



- **Key Issues:**
  - Nagaland's insurgency is deeply rooted in the demand for Naga **sovereignty and the creation of 'Greater Nagalim',** a unified Naga homeland encompassing Naga-inhabited areas across Nagaland, Manipur, Assam, Arunachal Pradesh, and parts of Myanmar.
  - Key groups include the National Socialist Council of Nagalim (Isak-Muivah) [NSCN-IM] and other factions like NSCN(K), NSCN(KN), and NSCN(R).
  - The issue is complicated by inter-tribal conflicts and the sensitivities of neighboring states regarding territorial integrity.
- **Approach:**
  - **Peace talks with the NSCN-IM** have been ongoing since 1997, marked by ceasefire agreements. However, a final resolution remains elusive due to persistent demands for a separate Naga flag and constitution, and the contentious 'Greater Nagalim' concept.
  - The government aims for an inclusive dialogue involving all **Naga factions** and the governments of neighboring affected states to find a solution within the **constitutional framework**. It also seeks to address the limitations of **Article 371A** concerning **land** and **resource ownership**.

Student Notes:

Tripura:

- **Key Issues:**
  - Historically, Tripura faced insurgency from groups like the **All Tripura Tiger Force (ATTF) and the National Liberation Front of Tripura (NLFT),** driven by ethnic tensions and demands for greater autonomy.
  - The state also dealt with the prolonged Bru-Reang refugee crisis, involving the displacement of thousands of tribal people.
- **Approach:**
  - Significant progress has been made through peace agreements. The **NLFT (SD) Agreement (2019)** led to the surrender of cadres and their reintegration.
  - The **Bru-Reang Agreement (2020)** resolved the 23-year-old refugee crisis by facilitating the permanent settlement of over 37,000 displaced individuals within Tripura, with substantial financial assistance from the central government. Consequently, Tripura is now largely free from active insurgency.

Meghalaya:

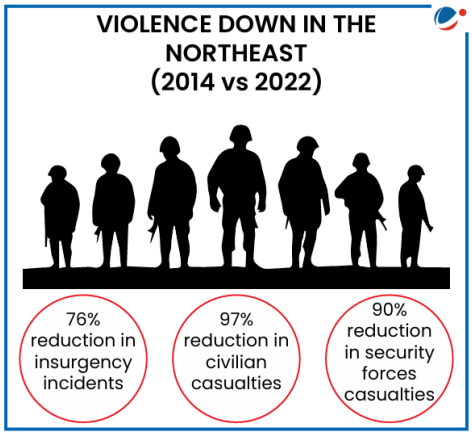
- **Key Issues:** Meghalaya has experienced insurgency, notably from **the Hynniewtrep National Liberation Council (HNLC),** which historically sought an independent Hynniewtrep homeland.
- **Approach:** The government has banned such groups under the **Unlawful Activities (Prevention) Act, 1967.** Through sustained security operations and peace initiatives, the state has largely brought insurgency under control, contributing to the overall improvement in the region's security situation.

Mizoram and Sikkim:

- **Key Issues:** These states have **largely remained free from significant insurgent activities**.
  - **Mizoram** successfully **resolved its long-standing insurgency** through the Mizo Peace Accord in 1986, which granted it statehood and significant autonomy.
  - **Sikkim** has historically enjoyed a peaceful environment.
- **Approach:** The relative peace in these states serves as a **model for conflict resolution through political dialogue** and the fulfillment of genuine aspirations within the Indian federal structure.

2.3. Approach to Handling Insurgency in NE

The government's strategy in the North-East has evolved into a **multi-pronged approach** encompassing proportionate use of force, dialogue, and structural changes.



- **Armed Forces (Special Powers) Act (AFSPA), 1958:** This act grants **special powers to armed forces in 'disturbed areas'** to maintain public order.
  - While deemed necessary by the state to tackle insurgency and prevent security gaps, it faces strong opposition due to allegations of human rights violations.
  - Recent Supreme Court rulings (e.g., 2016, 2017) emphasize minimum force and accountability, and various committees (e.g., Jeevan Reddy, Santosh Hegde) have recommended its repeal or stricter implementation.
  - As of July 2025, **AFSPA** remains in force in parts of **Nagaland**, **Manipur**, and **Arunachal Pradesh.**

- **Peace Process and Dialogue:** The Central Government actively pursues talks and negotiations with groups that abjure violence and seek solutions within the Indian Constitution. Numerous **Suspension of Operations (SoO) agreements and Memoranda of Settlements (MoS)** have been signed, leading to the dissolution of some outfits.
- **Scheme for Surrender-cum-Rehabilitation:** This scheme provides **financial assistance** (e.g., Rs. 4 lakhs immediate grant, Rs. 6000/month stipend for 3 years) and **vocational training** to militants who surrender, encouraging their reintegration into society.

UK's "Operation Banner" - Militarization Erodes Trust

The UK's **"Operation Banner"** in **Northern Ireland** (1969–2007) showed how long-term **militarization** can deeply damage **community trust**. The extended military presence, along with **controversial tactics**, ended up alienating a large part of the population.

This case clearly highlights the need for building **trust** in conflict situations, as excessive **military intervention** can unintentionally fuel **resentment** and **instability**.

- **Reimbursement of Security Related Expenditure (SRE):** This non-plan scheme reimburses states for expenses **incurred on security measures**, including training, logistics for CAPFs, ex-gratia payments to victims, and maintenance of designated camps for groups under SoO.
- **Civic Action Programmes (CAP): Implemented by Army and Central Armed Police Forces**, these programs undertake **welfare activities** (medical camps, sanitation drives, distribution of study material) to **build trust** and improve the image of security forces among local populations.
- **Modernization of Police Force:** The Scheme for Modernization of State Police Forces (MPF) aims to **upgrade police infrastructure, weaponry, communication, and training** to meet internal security challenges.
- **Border Management:** Measures include **construction of border fencing, floodlighting, and implementation of Comprehensive Integrated Border Management System (CIBMS)** with smart fencing (e.g., BOLD-QIT on Indo-Bangladesh border) to deter illegal infiltration.
- **Act East Policy:** This policy aims to **enhance connectivity, trade, and relations with Eastern neighbors,** with a focus on developing North Eastern states and improving their infrastructure.

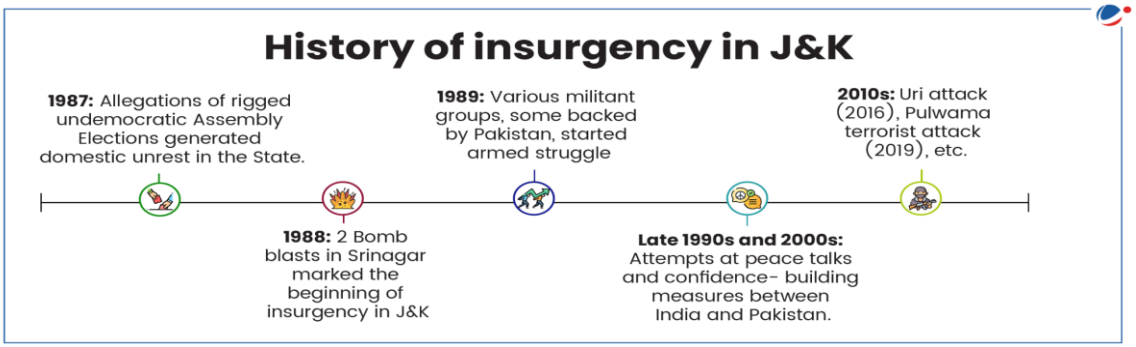
Student Notes:

3. Jammu and Kashmir Insurgency

The insurgency in Jammu and Kashmir (J&K) has evolved from a dispute over local autonomy into a significant internal security challenge.

3.1. Root Causes of Insurgency

- **Historical Context and Autonomy Dispute:** Despite accession to India in 1947, aspirations for independence persisted in the region since 1947. **Limited democratic development until the late 1970s** and the **reversal of reforms by 1988** curtailed non-violent expression of discontent.
- **Alleged Rigging of 1987 Assembly Elections:** This event is widely considered a **catalyst**, leading some legislative assembly members to form **armed insurgent groups** and contributing to anti-government sentiment.
- **External Sponsorship (ISI's Role):** Pakistan's Inter-Services Intelligence (ISI) has allegedly encouraged and aided the Kashmir independence movement, sponsoring terrorism to distract Indian troops and internationalize the issue. The **FBI in 2011 openly acknowledged ISI's role in sponsoring terrorism in Kashmir**.
- **Mujahideen Influence: Post-Soviet invasion of Afghanistan**, Mujahideen fighters infiltrated Kashmir, aiming to **spread radical Islamist ideology**, further complicating the conflict with strong Jihadist elements.
- **Sense of Alienation and Religious Marginalisation:** As India's only Muslim-majority state, a feeling of political, cultural, and economic marginalization compared to Hindus in the rest of India has fueled discontent.
- **Humanitarian Abuses: Accusations** of **humanitarian abuses and extrajudicial killings** by Indian troops operating under emergency powers have eroded public support for the government.

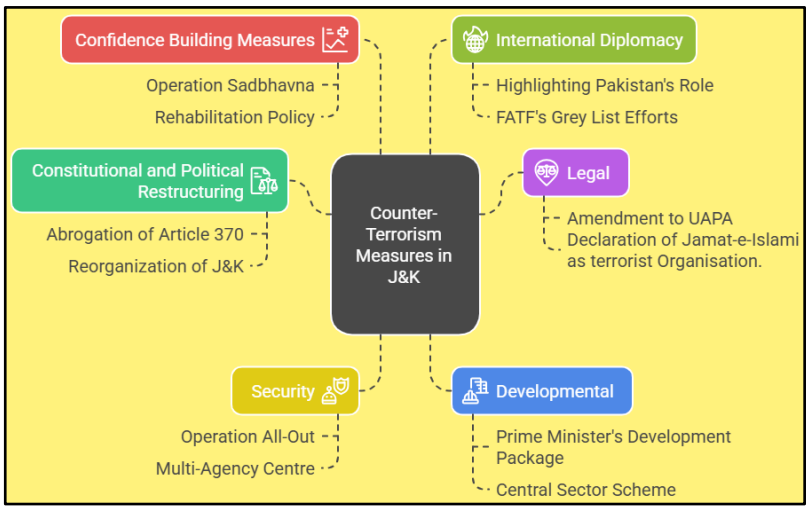


3.2. Approach to Handling Insurgency

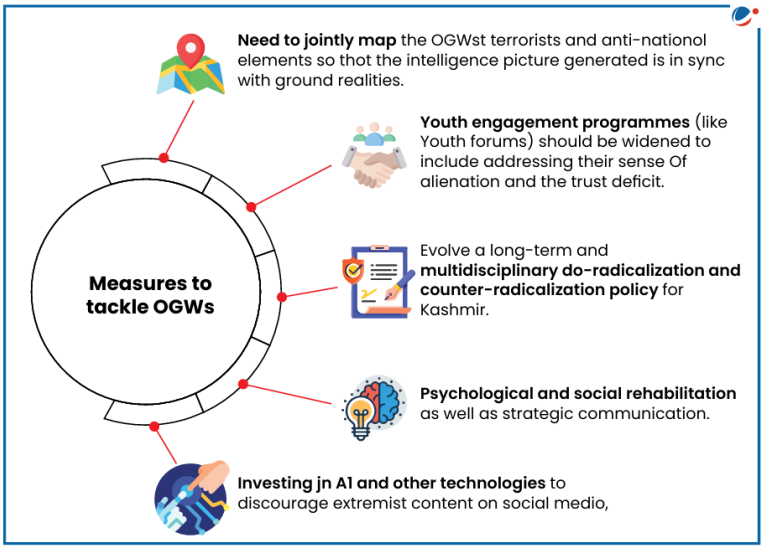
Student Notes:

India's response to the J&K insurgency has shifted from a **heavy-handed approach to a more nuanced strategy** emphasizing peacebuilding, development, and counter-terrorism.

1. **Security Measures:**
   - **Counter-Terrorist Operations:** Focus on **intelligence-based surgical operations**, reducing the presence of uniformed personnel in population centers, and ensuring transparency with zero tolerance for human rights abuses.



   - **Over Ground Workers (OGWs) Neutralization:** OGWs provide **logistical support, funding, ideological backing, radicalization, and recruitment for militants.**
     - Strategies involve categorizing OGWs (e.g., logistic support, funding, ideological support, recruitment, perception generation) and developing targeted responses.
     - This includes intelligence-based sting operations, psychological and social rehabilitation, strategic communication, and controlling social interactions (including digital) of OGWs.



     - Investing in AI and other technologies to discourage extremist content on social media is also crucial.
   - **Operation All Out:** Aims to **eliminate militant networks, OGWs, and top militant commanders**.
   - **Tackling Hybrid Terrorists:** Addressing the rise of **'part-time' or 'hybrid' terrorists** who are not officially listed but are radicalized and carry out small-scale attacks before returning to normal life.
2. **Developmental and Rehabilitation Initiatives:**
   - **UDAAN Scheme:** A **Special Industry Initiative** providing exposure and training to J&K graduates and post-graduates in corporate India, aiming to address unemployment.

Student Notes:

- **NISHTHA Scheme:** A **capacity-building program** for improving the quality of school education through integrated teacher training.
- **Himayat Mission:** Focuses on **generating sustainable livelihood opportunities** through self-employment and entrepreneurial skill development for J&K youth.
- **Rehabilitation and Surrender Policies:** Offer **facilities and incentives for terrorists who undergo a change of heart,** accept India's integrity, and are willing to return to the mainstream.
- **Economic Reconstruction:** Post-revocation of Article 370, efforts focus on attracting investments, extending social security measures (e.g., PM-KISAN, Atal Pension Yojana), and building transit accommodation for Kashmiri Pandits.

3. **Political and Governance Reforms:**
   - **Removal of Article 370 (2019):** This significant move converted the State of J&K into two Union Territories (J&K with an assembly, and Ladakh), abolishing its special status.
     - > **Positive Outcomes:** Extended reach of **Indian Constitution and laws** (e.g., RTI, RPA), new Domicile rules, decreased terrorism-related deaths, **fall in terrorist recruitment**, and fulfillment of Ladakh's aspirations.
     - > **Negative Outcomes:** Raised concerns about Kashmiri identity, severely affected education and economy due to shutdowns and **internet blockades**, increased cross-border infiltration attempts, and **internationalization** of the Kashmir issue.
   - **2024 assembly elections:** Recent elections in Jammu and Kashmir restored stability by enabling democratic governance, fostering public participation, and reducing alienation through legitimate political representation.
   - **Dialogue and Devolution: Dialogue** with state and non-state actors, demilitarization, and devolution of power to all three regions (Jammu, Ladakh, Kashmir) to prevent communal polarization.
   - **Restoring Trust:** Rebuilding trust in democratic machinery, addressing economic distress, lifting internet shutdowns, and robustly pushing education through scholarships and funding.

UNIT 2: ROLE OF EXTERNAL STATE AND NON-STATE ACTORS IN CREATING CHALLENGES TO INTERNAL SECURITY

"Terrorism is not a conventional war with standing armies... It exploits the seams of legal systems." – Robert Mueller

Previous Year Question

- **(2021)** Analyse the multidimensional challenges posed by **external state and non-state actors**, to the internal security of India. Also discuss measures required to be taken to combat the threats. (250 words)
- **(2019)** The **banning** of **'Jamaat-e – islaami'** in Jammu and Kashmir brought into focus the role of **over-ground workers (OGWs)** in assisting terrorist organizations. Examine the role played by OGWs in assisting terrorist organizations in insurgency affected areas. Discuss measures to neutralize the influence of OGWs.
- **(2019)** The **China-Pakistan Economic Corridor (CPEC)** is viewed as a cardinal subset of China's larger 'One Belt One Road' initiative. Give a brief description of CPEC and enumerate the reasons why India has distanced itself from the same.
- **(2016)** The terms **'Hot Pursuit'** and **'Surgical Strikes'** are often used in connection with armed action against terrorist attacks. Discuss the strategic impact of such actions.
- **(2014)** The diverse nature of India as a multireligious and multi-ethnic society is not immune to the impact of **radicalism** which has been in her neighbourhood. Discuss along with the strategies to be adopted to counter this environment.
- **(2014)** China and Pakistan have entered into an agreement for the development of an economic corridor. What threat does it pose for **India's security**? Critically examine.

1. External Threats to India's Internal Security

India's internal security challenges arise from both internal vulnerabilities and ongoing external efforts to create instability. These challenges are complex, with threats coming from both **conventional** and **non-conventional** external sources. The key **difference between threats** posed by a foreign entity and those from external sources that affect India's internal security is shown in the table below:

Conventional vs Internal Security Threats from External Sources

Category	Conventional External Threats	Internal Security Threats from External Sources
Nature of Threats	Acts of **military aggression** or **declared wars** between countries.	More **covert** threats, where external powers support **non-state actors** or **internal groups** causing unrest.
Method of Action	**Official armed forces** of a state directly involved in actions.	Uses **internal groups** or **non-state actors** to create problems, avoiding direct involvement.
Plausible Deniability	**No deniability**, as the actions are officially sanctioned by the state.	Allows the external state to **deny involvement**, avoiding direct responsibility.
Impact on India	**Clear and identifiable** external aggression.	**Internal instability** that complicates India's security situation.

Student Notes:

1.1. State Actors and Violent Non-State Actors (VNSAs)

The entities that perpetrate these threats can be broadly classified into two categories:

- **State Actors:** These are **governments and their official agencies,** such as the military or intelligence services, that use their resources to destabilize another nation.
  - A **prime example is Pakistan's Inter-Services Intelligence (ISI)**, which has been documented to fund, train, and direct terrorist operations against India.
- **Non-State Actors (NSAs):** These are **armed groups** that are wholly or partly independent of state governments and use **violence** to achieve their goals. The **South Asia Terrorism Portal** has listed over 180 such groups that have operated within India, many with transnational linkages. They include:
  - **Terrorist Groups:** Such as Lashkar-e-Taiba (**LeT**), Jaish-e-Mohammed (**JeM**), and global outfits like **ISIS** and **Al-Qaeda**.
  - **Insurgent Outfits:** Ethnic or secessionist groups, particularly in the North-East (e.g., NSCN factions) and Jammu & Kashmir.
  - **Organized Crime Syndicates:** Including drug cartels and human
  - trafficking networks, which often work in nexus with terrorist groups.

LeT: A Hybrid Terror Threat

Lashkar-e-Taiba (LeT) (Chief Hafiz Saeed) is a **Pakistan-backed Violent Non-State Actor (VNSA)**.

It uniquely blends a localized **insurgency** agenda, primarily focused on Kashmir, with a broader ideology of **global jihadism**.

This dual nature makes LeT a significant, complex threat. It operates as a **proxy** for **state interests** while simultaneously pursuing **international extremist goals**, posing challenges for both **regional and global security.**

Kinetic and **non-kinetic warfare** are strategic approaches used to target both **state** and **non-state actors**. While **kinetic warfare** focuses on the physical destruction of assets, **non-kinetic warfare** disrupts operations or morale through non-physical means, such as **cyberattacks** or **psychological operations**.

Aspect	Kinetic War	Non-Kinetic War
Nature	Direct physical force and violence, Highly visible (battlefield, news coverage) Immediate damage, casualties, infrastructure loss	Indirect, non-physical methods (psychological, cyber, etc.) Often covert or unattributed Long-term destabilization, societal/economic erosion
Means	Bullets, bombs, missiles, tanks, armed forces	Cyberattacks, disinformation, sanctions, electronic warfare
Actors	Primarily state militaries	States, non-state actors, hackers, proxy groups
Cost	High human, material, and financial costs	Lower direct cost but possible large long-term consequences
Examples	Airstrikes, invasions, artillery, direct combat	Cyber warfare, propaganda, sanctions, electronic jamming

Student Notes:

India's Geopolitical Landscape: Navigating a Volatile Neighbourhood

India is located in a **troubled and hostile neighborhood**, where many of its security problems trace back to the **1947 Partition**. Longstanding issues like the **Jammu & Kashmir** dispute, which is a "conflict of ideas" with **Pakistan**, and border disputes with **China** over areas like **Aksai Chin**, create a very tense environment.

External actors do not create conflicts out of a vacuum; they **exploit India's existing internal weaknesses** to destabilize the country. They use these existing fault lines to destabilize the country, providing **money, arms, and safe sanctuaries** to internal conflict groups:

- **Proxy War**: A strategy where an external power instigates or significantly supports a conflict while doing only a small portion of the actual fighting itself. This allows external actors to achieve their strategic objectives at a low cost.
- **Exploiting Fault Lines**: External state actors use **subversive propaganda** to amplify grievances among marginalized or disaffected groups within India.
- **Socio-Economic Disparities**: Grievances of **tribal populations** in Central India due to lack of development are exploited by **China**, allegedly providing **philosophical, financial, and intellectual support** to the Maoist movement.
- **Ethnic and Religious Tensions**: **Pakistan's ISI** has historically supported **Sikh militant groups** in their pursuit of **Khalistan** and has tried to exploit **communal fault lines** across India to radicalize youth and incite violence. This strategy of using **Non State Actors as proxies** allows external actors to destabilize India with minimal costs, famously referred to as **"bleeding India with a thousand cuts."**

The combination of unresolved historical conflicts, internal vulnerabilities, and external interference has made India's security situation **more complex and multifaceted** than that of many other nations.

2. Challenges from External State Actors

The challenges range from direct sponsorship of terrorism to a more subtle and sustained strategic encirclement.

2.1. Pakistan: The Epicenter of State-Sponsored Terrorism

Pakistan poses the most significant state-sponsored external threat to India's internal security. After failing in conventional wars, Pakistan adopted a state policy of **low-cost proxy warfare** against India. This strategy, famously known as **"bleeding India with a thousand cuts,"** is a form of **asymmetric warfare** designed to inflict continuous damage on India's security, economy, and social fabric without engaging in direct military conflict. This approach allows Pakistan to pursue its strategic goals while maintaining **plausible deniability**.

Terrorism's Asymmetric Calculus: Low Cost, High Impact

Terrorism provides an asymmetric cost-benefit scenario for those carrying out attacks. The **cost** of executing attacks is relatively low; for example, the **9/11 attacks** reportedly cost around **$500,000**. However, the **impact** is massive, creating immense **psychological fear** and significant **political disruption**.

The **9/11 attacks** alone cost the **US** around **$73 billion** in direct damages. **Globally**, counter-terrorism spending and the resulting **economic disruption** far exceed the initial attack costs, demonstrating how terrorism can cause severe **societal strain** with minimal investment.

Student Notes:

1. **The Architect of Terror: The "Deep State" and ISI**

   The execution of this proxy war is orchestrated by Pakistan's **"Deep State"**—a powerful nexus of its military and intelligence agencies.

   - The **Inter-Services Intelligence (ISI)** is the primary agency responsible for directing this strategy.
   - It actively handles the funding, training, and arming of various terrorist and insurgent groups that target India.

2. **Instruments of Violence: Nurturing Terror Proxies**

   The ISI has cultivated several terrorist organizations as strategic assets, with **Lashkar-e-Taiba (LeT)** and **Jaish-e-Mohammed (JeM)** being the most prominent. These groups **operate with impunity from Pakistani soil** and have been responsible for some of the most heinous attacks on India, including:

   - The 2001 **Parliament Attack**
   - The 26/11 **Mumbai Terror Attacks** (2008)
   - The 2019 **Pulwama suicide bombing**
   - **Pahalgam attack (2025)**

3. **A Multi-Front Assault on India's Security**

   Pakistan's strategy extends beyond specific terror attacks and targets multiple fronts to weaken India.

   - **Destabilizing Jammu & Kashmir:** Pakistan consistently fuels the conflict in the region by
     - Providing unwavering support to separatist and terrorist groups. Its tactics include **radicalizing local youth**.
     - Infiltrating foreign terrorists across the **Line of Control (LoC)**, and ensuring a constant supply of **arms and funds** to sustain the insurgency.
   - **Economic Warfare:** Pakistan also actively works to destabilize India's economy through a crime-terror nexus. This involves:
     - **Fake Indian Currency Notes (FICN):** Pushing high-quality counterfeit currency into India to finance terrorism and disrupt the economy.
     - **Narco-trafficking:** Leveraging its proximity to the **"Golden Crescent" (Afghanistan-Pakistan-Iran)** to facilitate drug trafficking into India.

Crypto-Terror: Funding Insurgency

Violent Non-State Actors (VNSAs), including groups like **ISIS**, increasingly use **cryptocurrencies** such as **Bitcoin**. This allows them to evade **state control** over financial transactions, facilitating illicit funding.

These digital currencies offer **anonymity**, **decentralization**, and **global reach.** This presents a significant challenge for **counter-terrorism financing**, making it harder to track and disrupt extremist funding networks.

2.2. China: An Ongoing Strategic Threat

China's challenge to India is strategic, long-term, and multi-dimensional, aimed at containing India's rise and undermining its stability. This threat manifests across several domains, from direct military pressure along the border to covert operations in the economic, cyber, and social spheres.

1. **Military and Border Threats: The Unresolved Frontier**

   The 3,488 km India-China border remains the world's longest disputed frontier and a primary flashpoint. China employs a strategy of **Grey-Zone Warfare**—coercive actions that fall below the threshold of conventional war—to exert pressure and alter the status quo.

Student Notes:

- **Grey-Zone Tactics on the LAC:** Along the **Line of Actual Control (LAC)**, China uses tactics like **"Salami Slicing"**, which involves the gradual capture of territory through minor transgressions and infrastructure construction in disputed areas.
    - This is complemented by **military intimidation** through aggressive patrolling and standoffs, exemplified by the **Doklam (2017)** and **Galwan Valley (2020)** incidents. The Galwan clash, the deadliest confrontation in decades, highlights the constant risk of escalation.
- **Military Modernization:** China's defense budget, which rose to $245 billion in 2025, heavily funds **high-altitude warfare** capabilities, advanced surveillance, and rapid infrastructure development in **Tibet** and **Xinjiang**, enabling swift troop mobilization along the LAC.
- **The Two-Front Challenge:** The deep, **"all-weather" strategic nexus** between China and Pakistan amplifies the risk of a **two-front challenge** for India.
    - A key element of this is the **China-Pakistan Economic Corridor (CPEC)**, a flagship project of the **Belt and Road Initiative (BRI)** that passes through **Pakistan-Occupied Kashmir (PoK)**. This directly undermines India's sovereignty and territorial integrity while solidifying the strategic encirclement.

2. Cyber and Hybrid Warfare: The Digital Battlefield

China has intensified its use of asymmetric tactics in the digital domain to achieve its strategic objectives without direct confrontation.

- **Escalating Cyberattacks:** Chinese state-linked hacking groups have increased their cyber operations against India's **critical infrastructure**, government agencies, financial institutions, and media through data theft, malware, and phishing campaigns.
- **Hybrid Threats:** Beijing employs **hybrid tactics** that merge digital and physical elements. These operations combine cyberattacks with sophisticated **disinformation** campaigns and support to proxy actors to foment unrest and destabilize India's internal environment.

3. Economic and Technological Leverage

China uses its economic influence as a tool for coercion and espionage, exploiting India's dependencies.

- **Economic Coercion:** India's reliance on Chinese imports in critical sectors like **electronics**, **telecom**, and **pharmaceuticals** (Active Pharmaceutical Ingredients or APIs) creates a significant vulnerability. Beijing can weaponize this dependency by restricting trade or manipulating supply chains.
- **Data Espionage and Tech Control:** Chinese commercial entities and mobile applications in India have been implicated in collecting personal and strategic data.
    - Investigations have revealed networks of **shell companies** used for economic espionage and influencing Indian firms through investments.
    - Furthermore, the dominance of Chinese firms in **telecom hardware** raises serious concerns about backdoor access and the potential for sabotage.

4. Support to Insurgency and Internal Destabilization

A key component of China's strategy is to fuel internal conflicts within India by providing support to various militant and extremist groups.

- **Northeast Insurgent Groups:** China has a long history of providing arms, training, financial support, and sanctuary to insurgent groups in Northeast India, including Naga (**NSCN**), Mizo, Meitei, and **ULFA** outfits. This support serves as leverage to keep the sensitive region destabilized.

- **Left-Wing Extremism (Maoists):** China is also believed to provide ideological, moral, and financial support to **Left-Wing Extremist (Maoist)** groups in India. By leveraging a shared Maoist ideology, it aims to brew internal security challenges and weaken the Indian state from within.

5. **Regional and Maritime Encirclement**

China is actively working to expand its strategic footprint in India's neighborhood, particularly in the maritime domain, to limit India's influence.

- **Indian Ocean Expansion:** China's growing naval presence in the **Indian Ocean**, including submarine deployments and access to ports in neighboring countries like Sri Lanka and Pakistan, is a core part of its **"String of Pearls"** strategy to encircle India and threaten its vital sea lanes of communication.
- **Regional Influence:** Through strategic investments and infrastructure projects like CPEC, China seeks to gain leverage over South Asian nations, further tightening its strategic encirclement of India.

2.3. Spillover Challenges from Other Neighbours

Significant security threats often spill over into India, not necessarily from state-sponsored action, but as a direct result of the internal instability and weak governance within neighboring countries.

1. **Myanmar: Porous Borders and Political Instability**

- **Porous Border**: The **1,643 km** long border with Myanmar, combined with dense forests, provides safe havens and operational bases for various **North-East insurgent groups**.

Decoding the "String of Pearls"

The **"String of Pearls"** is China's strategy to expand its influence in the **Indian Ocean Region (IOR)** by developing **ports** and **naval facilities** along key maritime trade routes, from **mainland China** to **Africa**.

India's Counter-Strategy: The "Necklace of Diamonds" : In response, India views this as a **strategic encirclement** and is pursuing the **"Necklace of Diamonds"** to protect its interests.

Port Development: India is securing ports like **Chabahar** (Iran) and **Sittwe** (Myanmar).

Strengthening Alliances: India has military access at **Oman's Duqm Port** and **Mauritius's Agalega Islands**, collaborating with **QUAD countries** (**USA**, **Japan**, **Australia**) to ensure a **free and open Indo-Pacific**.

Myanmar Nexus: Arms Flow to Northeast Insurgents

The **Chin National Army (CNA)**, a rebel group in Myanmar, operates in areas very close to the Indian border. A major security headache for India is the very real problem of **arms trafficking** that thrives across this **porous border**.

Weapons are frequently smuggled from Myanmar's conflict zones and end up in the hands of **Northeast Indian insurgents**. This constant flow of illegal arms highlights the serious **cross-border threats** India faces.

Student Notes:

Student Notes:

- **Political Instability**: The **military coup** in Myanmar has worsened the security situation, further destabilizing the region.
- **Rohingya Refugees**: The influx of **Rohingya refugees** from Myanmar presents security concerns, with fears of their **vulnerability to radicalization** by terrorist groups.
- **India's Response**: India has decided to **scrap the Free Movement Regime (FMR)** and **fence the border** to prevent cross-border threats.

2. **Bangladesh: Illegal Migration and Past Sanctuaries**

- **Illegal Migration**: Despite improved **security cooperation** with Bangladesh, **large-scale illegal migration** remains a significant challenge, especially in **Assam** and **West Bengal**. This has caused **demographic changes** and **ethnic tensions** in border states.

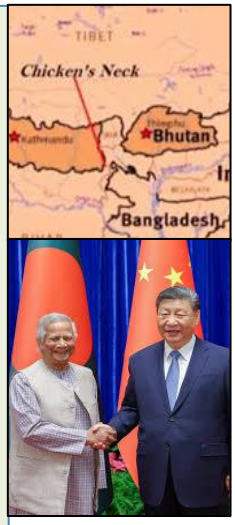
Spillover Risks from Neighbourhood Posturing: Bangladesh's Statement on Oceanic Leverage

In **March 2025**, Bangladesh's **interim leader Muhammad Yunus** referred to his country as the **"only guardian of the ocean"** for India's landlocked (the Chicken Neck Corridor) northeastern states, during an official visit to China.

By inviting **greater Chinese engagement in the region** and implying strategic leverage over India's connectivity, the statement was seen as **diplomatically provocative**.

Indian policymakers viewed this as a **concerning instance of neighbourhood rhetoric aligning with external powers**, potentially **complicating regional security and stability**.

The episode highlights how **political shifts in neighbouring countries** can **spill over into India's internal and strategic concerns.**



- **Past Sanctuaries**: In the past, **Indian Insurgent Groups (IIGs)** like **ULFA** used **Bangladesh** as a sanctuary, though the current government has cracked down on these groups.

3. **Nepal & Bhutan: Misuse of Open Borders**

- **Open Borders**: India shares open borders with **Nepal** and **Bhutan**, symbolizing friendly relations, but these borders are often misused by external actors.
- **Cross-Border Movement**: These borders serve as convenient **transit routes** for **terrorists**, **criminals**, and **smugglers**, facilitating the movement of **arms**, **Fake Indian Currency Notes (FICN)**, and **narcotics** into India.
- **ISI Activities**: Pakistan's **ISI** has a history of using this vulnerability for its **anti-India operations**. Two key examples prove this point:
  - In **December 1999**, terrorists hijacked flight **IC 814** after it departed from Nepal.
  - In **August 2013**, Indian Mujahideen terrorist **Yasin Bhatkal** was captured near the India-Nepal border after using it to hide.

3. Challenges from Non-State Actors

India faces significant security challenges from a wide variety of non-state actors operating both within and across its borders. These groups fuel everything from organized crime and internal insurgencies to deadly cross-border terrorism.

- **Terrorism**: Over **180 terrorist groups** have operated in India. **Lashkar-e-Taiba (LeT)** and **Jaish-e-Mohammed (JeM)**, originating from **Pakistan**, have carried out major attacks, such as the **2008 Mumbai attacks** and **Pulwama attack** in 2019.

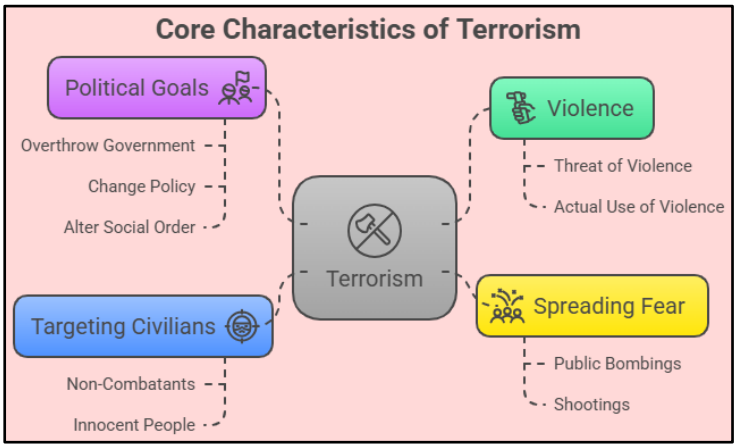
Student Notes:

- **Left-Wing Extremism**: **Maoist groups** such as the **CPI (Maoist)** operate in **Chhattisgarh**, **Jharkhand**, and **Odisha**, obstructing **development** by targeting government projects and spreading **propaganda** to recruit vulnerable youth.
- **Insurgency in the Northeast**: **Groups** like the **United Liberation Front of Assam (ULFA)** and **Nationalist Socialist Council of Nagaland (NSCN)** fuel insurgency in the **Northeast** due to **inter-tribal conflicts** and **illegal migration** from **Bangladesh**, creating an environment conducive for **non-state actors**.
- **Drug Trafficking**: India's proximity to the **Golden Triangle** (Myanmar, Laos, Thailand) and **Golden Crescent** (Afghanistan, Pakistan, Iran) makes it vulnerable to drug trafficking. For example, **heroin** is smuggled into India through **land borders** with **Myanmar** and **Afghanistan**, while **sea routes** from the **Indian Ocean** are also exploited.
- **Human Trafficking**: Despite being illegal, **human trafficking** remains a major issue. For instance, **Nepalese women** are often trafficked through India for **commercial sexual exploitation**, and **Bonded Labour** is widespread in industries like **brick kilns** in states like **Tamil Nadu** and **Andhra Pradesh**.
- **Civil Society Organisations**: **Foreign-funded NGOs** in Kerala and Kochi have been reported to be **involved in protests** against the Kochi Marina Project, raising concerns about external influence.

Although state actors pose a strategic threat, the most direct and frequent challenges to India's internal security arise from **Violent Non-State Actors (VNSAs)**. The primary form of this threat is **terrorism**, which the upcoming section will explore in detail.

3.1. Terrorism

3.1.1. The Challenge of Defining "Terrorism"



Defining **terrorism** remains controversial and difficult, as the term is often shaped by political, ideological, or strategic biases. The core dilemma is that **"one person's terrorist is another person's freedom fighter"**—what qualifies as terrorism depends largely on perspective.

Importantly, most frameworks do **not define terrorism as a concept**, but rather **describe specific acts** considered terrorist in nature based on **intent and effect**.

International Framework: UN General Assembly Resolution 49/60: The **UNGA Resolution 49/60 (1994)** does not define terrorism per se but criminalizes certain acts widely seen as terrorist. It states:

"Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them."

This description focuses on the **intent to spread fear for political purposes**, dismissing any ideological justification.

Indian Legal Framework: Bharatiya Nyaya Sanhita, 2023: The **Bharatiya Nyaya Sanhita (BNS), 2023**, similarly refrains from defining terrorism directly. Instead, it classifies a **terrorist act** as:

*Any act intended to **threaten the unity, integrity, sovereignty, or economic security of India**, or to **strike terror in the people**, typically involving the use of **violence for ideological or social objectives**.*

This approach prioritizes **national security and public fear** as key indicators of terrorism, irrespective of the actor's motivation.

3.1.2. Classifying Terrorist Threats in the Indian Context

Terrorism in and around India is a complex issue, with different categories based on the actors and motivations:

- **State-Sponsored Terrorism**: This involves a foreign government supporting terrorist groups, providing **safe heaven, financial aid**, **military training**, and **ideological justification**. A major example is **Pakistan's support** for groups like **Lashkar-e-Taiba** and **Jaish-e-Mohammed**.
- **Violent Non-State Terrorism**: Carried out by **armed groups** not affiliated with any government. These include **narcotics cartels** and **ideologically driven groups** like **paramilitary militias**.
- **Ethno-Nationalist Terrorism**: The goal here is to create a separate state for a particular ethnic group or to elevate one ethnic group over others. This form of terrorism has been a major challenge in India. Examples include:
    - The insurgency in **Jammu & Kashmir**, driven by secessionist groups often supported from across the border.
    - The **Khalistan movement** in Punjab during the 1980s, which demanded a separate Sikh state.
    - Various insurgent groups in **Northeast India** fighting for independence or autonomy.
- Tamil Nationalist groups like the **LTTE** in Sri Lanka.

Different Types of Terrorism

Terrorists adapt their tactics to exploit modern vulnerabilities:

Cyber-Terrorism: Involves using **information technology** to attack critical infrastructure, like **hacking** government networks or **disrupting** financial markets, causing fear without physical bombs.

Narco-Terrorism: Links **drug trafficking** with terrorism. **Drug cartels** use violence to influence governments, while **terrorist groups** fund their operations through **narcotics sales**.

Bio-Terrorism: The intentional release of **biological agents** like **viruses** or **bacteria** to harm and scare populations. High-threat agents include **Anthrax**, **Smallpox**, and **Plague**.

Nuclear Terrorism: The most dangerous form, involving attacks on **nuclear power plants**, the use of a **dirty bomb**, or acquiring **nuclear weapons** to cause widespread destruction.

Key characteristics of Terrorist Organizations

Political/Ideological Motives: Terrorist organizations primarily aim to gain **power** through political, **religious**, or **ethnic** means, using violence.

Use of Violence: **Violence** is central to their operations, which often involve **mass casualties** and **attacks on infrastructure**.

Visibility: These groups often claim responsibility for their actions to gain **public support** and demonstrate their **commitment** to their cause.

Confrontation with State: Their central goal is to **overthrow** or **destabilize** existing governments through violent **struggle**.

Structure: Terrorist groups may operate in **cellular structures**, making them **difficult to infiltrate** by security agencies.

3.1.3. India's Two-Front War on Terror

India continues to face significant and evolving security threats from terrorist organizations operating from beyond its borders. These groups can be broadly divided into those sponsored by neighboring states and larger, global networks.

1. **The Enduring Threat from Pakistan-Backed Groups**

   For decades, India has been the target of terrorism from groups based in **Pakistan**. Organizations like **Lashkar-e-Taiba (LeT)**, **Jaish-e-Mohammad (JeM)**, and **Hizb-ul-**

Student Notes:

Student Notes:

Mujahideen (HM) operate with significant **financial**, **logistical**, and moral support from elements within the **Pakistani establishment**.

These groups have a long and brutal history of carrying out deadly attacks, not just in **Jammu & Kashmir**, but in major cities across the country. Some of the most infamous incidents include:

- The **2001 Parliament Attack** in Delhi.
- The horrific **2008 Mumbai Attacks (26/11)**, a three-day siege that killed over 170 people.
- The deadly **2019 Pulwama Attack**, where a suicide bomber killed 40 CRPF personnel.

The nature of this threat continues to evolve. In a recent and alarming development on **April 22, 2025**, militants attacked a village in **Pahalgam**, J&K, killing 26 people, including 25 Indian tourists. The attack was claimed by **The Resistance Front (TRF)**, which is widely considered a front organization or proxy for **LeT**. **This incident signaled a dangerous shift towards targeting civilians to spark communal tension in India.**

In a firm response, India launched **Operation Sindoor** on May 7, 2025. This decisive military action targeted nine terror camps belonging to **LeT**, **JeM**, and **HM** inside Pakistan and Pakistan-occupied Kashmir, hitting key operational hubs like **Muridke** (LeT headquarters) and **Bahawalpur** (JeM headquarters).

Combating Online Radicalization: EU's Model

The **European Union** provides a strong **model for India** on how to tackle **online terrorist propaganda**. Through units like **Europol's Internet Referral Unit**, the EU actively works with **tech companies** to quickly find and remove harmful content from groups like ISIS.

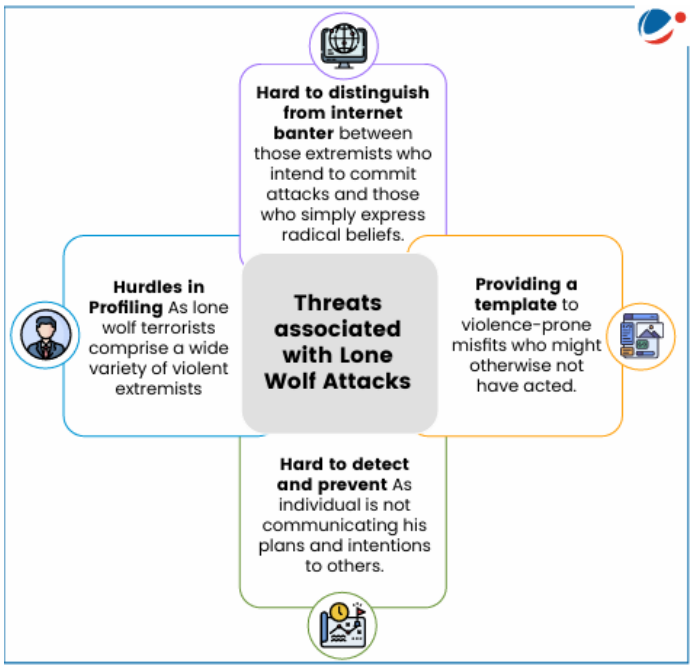
This effort is backed by powerful laws like the **Terrorist Content Online (TCO) Regulation**, creating a structured system for **social media monitoring** that helps counter radicalization effectively.

2. The Growing Influence of Global Terror Networks

Beyond the immediate threat from **Pakistan**, India also faces challenges from **transnational jihadist organizations** like **Al-Qaeda** and the **Islamic State (ISIS)**, particularly its regional branch, the **Islamic State Khorasan Province (ISKP)**.

Modus Operandi:

- **Online Radicalization:** These groups use **social media** and **encrypted messaging apps** to **radicalize** and **recruit** vulnerable youth through high-quality **propaganda** in regional languages. They also disseminate **bomb-making manuals** and plan operations through the **darknet**.
- **Lone Wolf Attacks**: These organizations encourage individuals to carry out **self-radicalized** attacks with minimal intelligence footprint. A "lone wolf" is an individual who is radicalized—often online—



Student Notes:

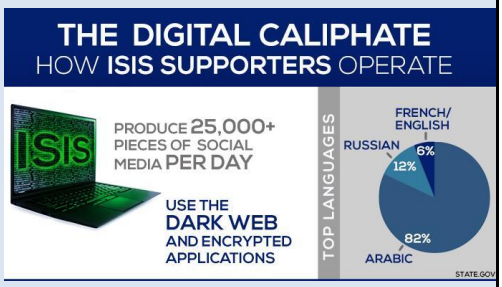
and commits violent acts alone, without direct command or material support from a larger group. These attacks are extremely difficult for security agencies to detect and prevent.

- They remain a concern due to the **volatile neighborhood**, access to **social media**, and the **youth population** vulnerable to radicalization.
- While India's strict gun laws make it harder for lone wolves to acquire sophisticated weapons, the use of vehicles, knives, and homemade explosives remains a potent threat.

Indian security agencies have successfully **foiled several plots** and arrested ISIS sympathizers in states like **Maharashtra**, **Kerala**, **Telangana**, and **West Bengal**. Furthermore, **Al-Qaeda in the Indian Subcontinent (AQIS)** has attempted to establish cells in Assam and West Bengal.

While the direct operational capability of these global groups in India remains limited compared to the Pakistan-backed outfits, the threat from their **sleeper cells** and persistent **online radicalization** efforts remains a serious and ongoing concern.

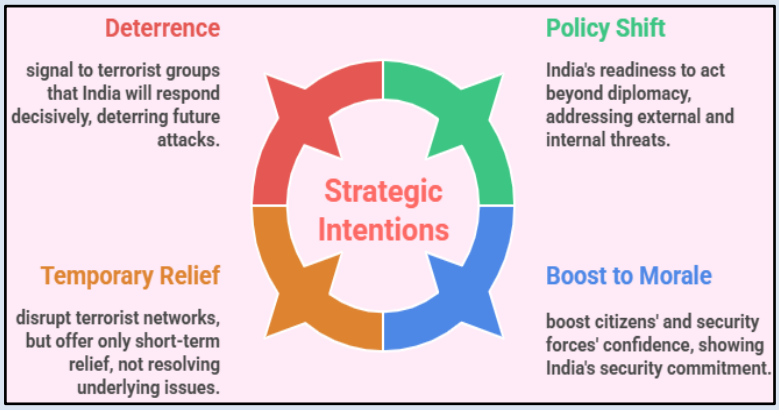
Cyber Caliphate: ISIS's Digital Warfare



ISIS consistently utilizes platforms like **Telegram** for **online radicalization** and **recruitment**, a verified global tactic. India has genuinely seen instances where individuals, notably from **Kerala**, have been influenced by such digital propaganda.

This highlights a critical **internal security challenge**: how digital networks are exploited to draw **youth** into extremism. Combating this demands continuous **social media monitoring** and robust counter-narrative strategies to prevent radicalization.

Covert Operations, Pre-emptive Strikes, and Surgical Strikes: Strategic Approaches in India's Internal Security



The strategic responses, such as **covert operations**, **pre-emptive strikes**, and **surgical strikes**, play a vital role in **India's counterterrorism strategy**, complementing broader efforts to safeguard national security and maintain regional stability.

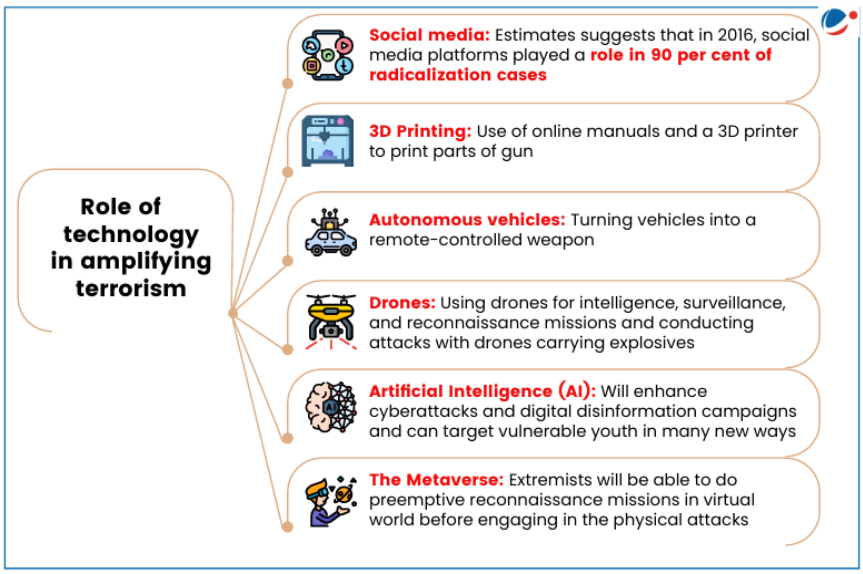
- **Covert Operations**: Secret missions conducted to achieve objectives without direct attribution or open involvement by the state. These operations are designed to remain undetected and achieve strategic goals.
- **Pre-emptive Strikes**: Attacks launched to neutralize imminent threats before they can result in harm, preventing attacks before they occur.
- **Hot Pursuit**: A military or law enforcement action where forces chase and attack **terrorists** or **criminals** across borders without waiting for permission, often in response to an ongoing threat.

- **Surgical Strikes**: Carefully planned, targeted attacks, typically on **terrorist camps** or specific threats, designed to minimize **collateral damage** while achieving precise objectives.

Student Notes:

3.1.4. The Modern Playbook of Terrorism: New Threats and Emerging Challenges

Terrorism today has transformed into a global, fast-moving threat. It no longer relies solely on traditional methods. Modern terrorists have adopted a sophisticated playbook that leverages technology, exploits urban vulnerabilities, and blurs the lines between crime, terror, and warfare.



3.1.4.1. Hybrid Threats: Technology as a Weapon

Technology is the central nervous system of modern terrorism.

The Digital Battlefield

The **digital domain** has become a primary battleground for a new kind of war, with adversaries leveraging various tactics to destabilize societies. Terrorist organizations use digital tools for every aspect of their operations, turning the internet into a primary battlefield. The core principle is simple: **a terror act is a message,** and technology is the ultimate megaphone to broadcast that message to a global audience.

- **Propaganda and Recruitment:** Social media platforms and encrypted messaging apps are used to spread extremist ideology. High-quality videos, online magazines, and AI-generated content like **deepfakes** are used to justify violence, radicalize vulnerable youth, and recruit new members. It's estimated that social media plays a role in up to **90% of radicalization cases**.
- **Financing and Planning:** The internet makes it easy to raise and move funds through online payment systems, cryptocurrencies, and fundraising for seemingly legitimate charities. Encrypted communication allows terrorist cells across different continents to plan attacks securely.

Student Notes:

- **Training and Execution:** Groups provide online manuals and instructional materials for everything from bomb-making to counter-intelligence and hacking.
- **Use of Social Media for Disinformation and Psychological Warfare**:
  - **Weaponizing information**: Adversaries are using social media platforms to run **coordinated disinformation campaigns**, spread **fake news**, and propagate **divisive narratives**.
  - **Psychological warfare**: These tactics aim to create **social discord**, undermine trust in state institutions, and **polarize society**, weakening the national fabric from within.

- **Cross-border Cyber Attacks on Critical Information Infrastructure (CII)**:
  - **Cyber threats**: **State-sponsored hackers** and **cyber-terrorists** pose significant risks to **India's Critical Information Infrastructure (CII)**, which includes sectors like **banking**, **power grids**, **transport**, and **healthcare**.
- **The Challenge of Deepfakes and AI-generated Content**:
  - **Emerging technologies**: The rise of **Artificial Intelligence (AI)** has introduced new threats, including **deepfakes**—AI-synthesized videos or audio that can create highly convincing but false content.
  - **Impact**: These can be used for **sophisticated propaganda**, **defaming public figures**, or fabricating **false evidence** to incite **social unrest**, making it increasingly difficult to distinguish fact from fiction.

The Drone/UAV Threat

The use of **low-cost, commercially available Unmanned Aerial Vehicles (UAVs) or drones** has added a new and dangerous dimension to cross-border threats.

- **Use of Drones for Cross-border Smuggling**
  - **Adversaries**, particularly from **Pakistan**, are increasingly using **drones** to smuggle **arms**, **ammunition**, and **narcotics** across the border into **Punjab** and **Jammu & Kashmir**.
  - The **small size** and **low flight altitude** of these drones make them difficult to detect using **conventional radar systems**, allowing them to operate with relative ease
- **The Potential for Weaponized Drones**
  - Beyond **smuggling**, there is a growing threat of drones being **weaponized**.
  - Drones can be **modified** to carry **Improvised Explosive Devices (IEDs)**, posing a significant risk to **security installations**, **critical infrastructure**, and **public gatherings**, as demonstrated in conflict zones worldwide.

India's Initiatives to Tackle Drone Threats

- **Counter Drone System (D4 System)**: Developed by **DRDO** and **Bharat Electronics**, the **D4 system** detects, tracks, and neutralizes **micro/small UAVs**.
- **Anti-Rogue Drone Technology Committee (ARDTC)**: **Ministry of Home Affairs** established **ARDTC** to evaluate, **certify counter-drone technologies**, ensuring effectiveness in dealing with **rogue drone** threats.
- **Deployment of Anti-Drone Systems at Borders**: **D4 systems** and **Netra drones** are deployed along **Indo-Pak** and **Jammu & Kashmir borders** to counter **smuggling** and **terrorist drone activities**.
- **Detailed Vulnerability Mapping**: **Vulnerability mapping** along the **Indo-Pak border** uses **specialized vehicles**, **infrared sensors**, and **cameras**.
- **National Counter-Rogue Drone Guidelines (2019)**: **National Counter-Rogue Drone Guidelines** provide a **framework** for **drone detection**, **registration**, and issuing **Unique Identification Numbers (UINs)** for regulation.
- **Very Short Range Air Defence System (VSHORAD)**: **VSHORAD** is an **indigenous missile system** designed to **intercept** and **destroy** low-altitude **aerial threats**, including **drones**, like **SAMAR-1** and **Igla-S**.

Student Notes:

Asymmetric warfare using Low cost Drones

Low-cost drones have completely changed the rules of **modern warfare** for instance:

- **Houthi rebels** used cheap drones to successfully attack a U.S. ship, forcing the American military to spend over a billion dollars on expensive missiles just to shoot them down.
- In the **Ukraine war**, simple **commercial drones** fitted with **grenades** are being used for deadly attacks and **reconnaissance** against advanced armies.

The **U.S.-owned ship Genco Picardy** after it came under **attack from** a bomb-carrying drone launched by **Yemen's Houthi** rebels

This creates a huge problem for powerful **militaries**, which are built to fight other big nations, not swarms of inexpensive drones. To counter this, countries are now racing to develop cheaper, **cost-effective counter-drone solutions**.

Drone Warfare During Operation Sindoor

During the conflict surrounding **Operation Sindoor**, **drones** became the main weapon for both India and Pakistan. This was the first time unmanned systems played such a central and coordinated role in a conflict between the two nuclear-armed neighbors, marking a new chapter in modern warfare.

India's Drone-Led Offense

From the very beginning of **Operation Sindoor**, India integrated drones into its attack plans. The initial strikes on terror camps were supported by **loitering munitions** (also called **kamikaze drones**) to ensure precision and effectiveness.

- The initial assault included the use of **SkyStriker suicide drones**, which carry a 10kg warhead.
- As the conflict escalated, India retaliated against Pakistani aggression by using advanced Israeli-made **Harop drones** to destroy key Pakistani air defence and radar sites.

Pakistan's Mass Drone Counter-Attack

Pakistan's response, named **Operation Bunyan al-Marsus**, was a massive drone-led assault.

- In a major offensive between May 8th and 9th, Pakistan launched an estimated **300-400 drones** from **36 different locations**.

- These were likely Turkish-made **Asisguard Songar drones** and were used to target Indian military installations across a wide area, including in Jammu & Kashmir, Punjab, Rajasthan, and Gujarat.

The Defensive Battle

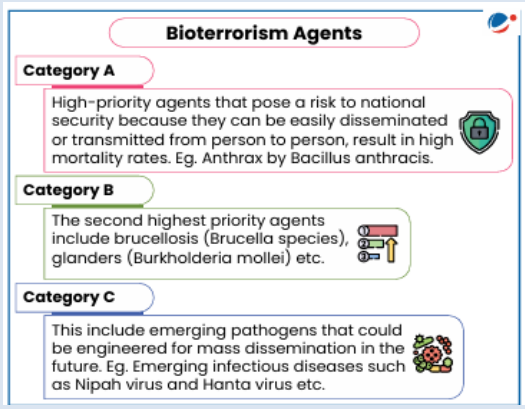
To defend against this large-scale drone attack, India activated its **Integrated Counter-UAS (Unmanned Aerial Systems) Grid**. This created a powerful, multi-layered defensive shield using a combination of systems:

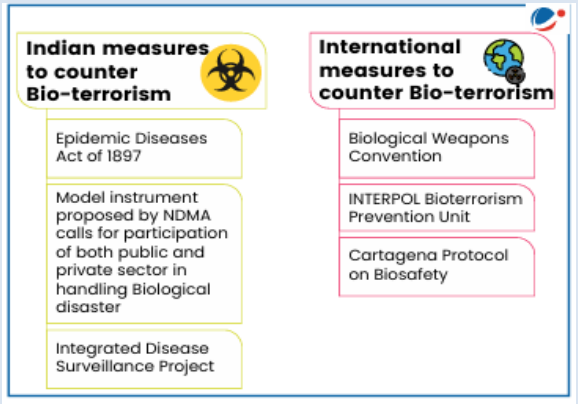
- The Russian **S-400 Triumf** long-range system.
- **India-Israel** jointly developed **Barak-8 MRSAM**.
- The indigenous **Akash** missile system.
- India also used its own **Harpy drones** in a counter-attack role.

This drone war highlights a major shift in modern conflict. Both countries used drones as a less risky first step than sending manned jets, allowing them to test each other's defenses.

India's efforts to combat drone threats include **public awareness campaigns** in **border areas**, encouraging citizens to report suspicious activities, and **international collaboration** for **intelligence sharing**. To further enhance security, India could invest in **advanced drone detection systems**, establish **dedicated drone response units**, improve **regulatory frameworks**, and increase **research and development** for innovative **anti-drone technologies**, ensuring comprehensive defense against evolving drone threats.

Bio-Terrorism





3.1.4.2. Shifting Battlegrounds: From Borders to Cities and Individuals

While border regions remain volatile, the focus of modern terrorism has increasingly shifted to cities and towns, a phenomenon known as **Urban Terrorism**.

Why Cities are Prime Targets:

- **Anonymity and Logistics:** The diverse and dense population of cities provides anonymity, making it harder to detect terrorists. Logistical needs like transportation, communication, and arms are also more readily available.
- **High-Impact Targets:** Cities contain critical infrastructure, mass gatherings, and symbolic landmarks. Attacking these maximizes casualties and media attention, spreading fear more effectively. The **2008 Mumbai attacks** are a classic example of a coordinated urban terror assault.
- **Media Amplification:** With a heavy concentration of print and electronic media, cities guarantee that the "propaganda by the deed" is broadcast instantly and widely.

Student Notes:

Lone Wolf Terrorism in India: Coimbatore & Bengaluru Cases

India is facing a growing threat from **lone wolf terrorism**, where individuals, radicalized in isolation, carry out attacks on their own.

Recent incidents like the **Coimbatore car explosion** (October 2022) near a temple and the **IED blast** at Bengaluru's **Rameshwaram Cafe** (March 2024) highlight this dangerous trend. In both cases, a single attacker operated with minimal external support, using homemade bombs to target civilians.

These **lone wolf** attackers are a major challenge because they are incredibly difficult to detect. Fueled by **online extremist content**, they operate without a group, making them **elusive yet dangerous** to internal security.

3.1.4.3. The Invisible Ecosystem of Terror: Over-Ground Workers and Sleeper Cells

1. **Over-Ground Workers (OGWs)**

   The network of **Over-Ground Workers (OGWs)** is the invisible logistical and ideological backbone that sustains terrorism and insurgency on the ground.

   - **OGWs as the "Eyes and Ears" and Logistical Backbone**
     OGWs are not armed combatants, but they are essential for the survival and operations of terrorist organizations. Operating under **civilian cover**, they act as the **"lifeline"** for these groups, linking **underground cadres** with the **local population**. Their covert nature makes them difficult to identify and prosecute.

Pulwama's (2019) Hidden Facilitators: The OGW Network

The **2019 Pulwama attack** unequivocally highlighted the critical role of **Over-Ground Workers (OGWs)**.

Investigations into this specific incident confirmed OGWs, the **logistical backbone** for terrorists, provided the **explosives-laden car** and crucial support like shelter for the perpetrators.

Student Notes:

2. Sleeper cell

A **sleeper cell** is a hidden group of **terrorists** or spies who live normal, unnoticed lives within a community. They remain inactive for years until they are "activated" by overseas **handlers** to carry out attacks, gather intelligence, or provide support for operations.

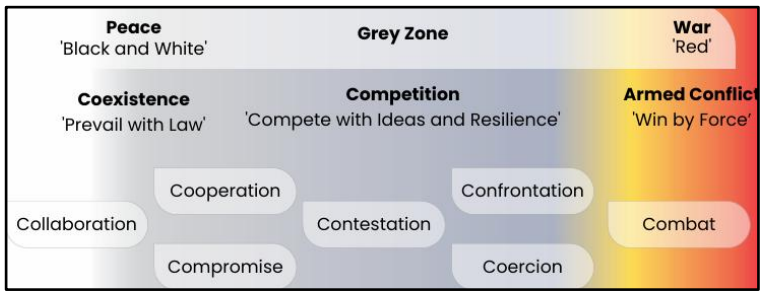
- **Delhi ISI Sleeper Cell (2025):** Delhi Police arrested two ISI agents, including a Nepali national, for leaking sensitive military information to Pakistan.
- **ISIS Sleeper Cell in Pune (2023–2025)**: NIA arrested two radicalized Indians linked to an ISIS module that conducted bomb-making workshops and planned terror attacks.

These **sleeper cells** are extremely difficult to detect because their members blend in so well with the local population. They often use **encrypted communication** and engage in long-term planning, posing a serious and widespread challenge to India's internal security.

3.1.4.4. The Blurring Lines: Grey-Zone Warfare

One of the most complex challenges today is **Grey-Zone Warfare**, which involves the use of unconventional tactics that fall just below the threshold of traditional war. The goal is to weaken an adversary without triggering a full-scale military response.

Key Tools of Grey-Zone Warfare:



- **Cyber Operations:** Hacking critical infrastructure, such as the 2020 cyberattack on the **power grid in Maharashtra**.
- **Information Warfare:** Using propaganda, fake news, and social media manipulation to create social division and undermine trust in government.
- **Economic Coercion:** Imposing trade restrictions or manipulating markets to damage a target nation's economy.
- **Support to Proxy Forces:** This is a classic tactic where a state supports non-state actors like insurgents or terrorists to fight on its behalf.

Pakistan's **"Deep State"** (influential elements within its military and intelligence agencies) has historically used terrorism as a foreign policy instrument, nurturing groups like **Lashkar-e-Taiba (LeT)** and **Jaish-e-Mohammed (JeM)** as strategic assets against India. This is a prime example of grey-zone conflict through proxy forces.

3.1.4.5. Evolving Threats: From Military Targets to Civilians in Jammu & Kashmir

Over the past five years, Jammu & Kashmir (J&K) has witnessed a troubling shift in terrorism patterns, with increasing attacks on **civilians** and **tourists**. These incidents have primarily targeted **religious minorities** and **non-local visitors**, indicating a new strategy by militants to create **communal divisions** and disrupt the region's economy, particularly **tourism**.

Targeting Religious Minorities and Tourists

- **Sectarian Attacks**: Terrorists have deliberately targeted **Hindu** and **Sikh minorities**, as well as **tourists** visiting pilgrimage sites. The attacks often single out victims based on their **religious identity**, as seen in the **2025 Pahalgam massacre**, where **Hindu** tourists were separated and executed based on religion.
- **Tourism Under Attack**: **Tourism** has been a frequent target, especially during the spring and summer months, a crucial time for the local economy. Attacks on **hotels**, **pilgrimage convoys**, and **travel routes** have been aimed at derailing efforts to revive tourism in the region.

Student Notes:

Year	Major Attack/ Incident	Location	Target	Key Features
2017	Amarnath Yatra massacre	Anantnag, J&K	Hindu pilgrims (Amarnath Yatra)	Bus ambushed; 8 killed, 18 injured; LeT blamed
2021	Series of attacks on minorities	Various (J&K)	Minorities, migrant workers	Attacks near temples and transit points
2024	Reasi bus attack	Reasi district, Jammu	Hindu pilgrims	Ambush; bus plunged into gorge; 9 killed, 41 injured
2025	Pahalgam massacre	Pahalgam, Kashmir Valley	Hindu, Christian tourists	Religion-based segregation and killings; 26 killed

Geographic Shifts

- **Increased Attacks in Jammu**: While violence in the **Kashmir Valley** declined after 2019 due to increased security, there has been a rise in attacks in **Jammu**, which is known for its **communal diversity**. Militants exploit local tensions in this region, often time their attacks to disrupt **political** or **religious events**.

Psychological and Communal Impact

- **Psychological Warfare**: Terrorists aim to generate **fear** and **trauma** by attacking civilians, especially tourists, to create **communal polarization**. The **2025 Pahalgam massacre** exemplified this, with survivors being forced to narrate their traumatic experiences to political leaders, amplifying the communal message.
- **Displacement and Fear**: These targeted attacks have caused significant **trauma** to survivors, particularly those from outside Kashmir, leading many to reconsider their **travel plans**. This, in turn, affects both **tourism** and **inter-community relations**.

3.1.4.6. Mobilization of Diaspora for Terrorism

Khalistan terrorism, which originated from the demand for a **separate Sikh homeland** in Punjab, has seen a resurgence due to **diaspora support** in recent years. While largely suppressed within India, the **Khalistani movement** has gained momentum abroad, primarily driven by **online radicalization** and **funding** from **overseas Sikh communities**.

Diaspora-Led Radicalization and Funding

- **Radicalization through Social Media**: Khalistani extremist groups, such as **Sikhs for Justice (SFJ)**, **Babbar Khalsa International (BKI)**, and the **World Sikh Organisation**, use **online campaigns**, **community centers**, and **social media** to spread the separatist ideology and recruit youth, particularly from the Sikh diaspora.
- **Funding Channels**: These groups raise funds through **international charities**, **community events**, and donations, funnelling money into extremist activities in India.

Canada's Extremist Base

The **Canadian Security Intelligence Service (CSIS)** officially confirms **Khalistani extremists** are actively using **Canadian soil** as a base. They engage in **promotion, fundraising, and planning violence**, primarily targeting **India**.

This significant acknowledgement validates India's long-standing concerns, highlighting an ongoing **national security threat** stemming from Canada-based extremist activities.

Global Pro-Khalistan Mobilization and Referendums

- **Khalistan Referendums**: **SFJ** and other pro-Khalistan groups have organized **unofficial Khalistan referendums** in several countries, particularly in **Canada**, the **UK**, and the **US**. These events aim to **internationalize** the Khalistan issue but have also sparked **violent clashes** with opposing communities.

Student Notes:

Attacks on Indian Diplomatic Missions and Vandalism

- **Vandalism and Protests Abroad**: Pro-Khalistan activists have **vandalized Indian embassies** in cities like **London**, **Ottawa**, and **San Francisco**, desecrating the **Indian flag** and other symbols. **Hindu temples** in areas with large **Sikh populations** have also been targeted.

Case Study: D-Company and ISI – A Snapshot of the Crime-Terror Nexus

The growing convergence between **organized crime and terrorism** poses a serious threat to national security. This relationship exists along a **crime-terror continuum**, ranging from loose cooperation such as providing fake documents or transport, to complete confluence where criminal and terror operations overlap.

A striking example is the **1993 Mumbai serial blasts**, which illustrate a deadly collaboration between:

- **D-Company**, the crime syndicate led by Dawood Ibrahim, which used its smuggling networks to bring RDX via the coast and arrange logistics for the attack.
- **Pakistan's ISI**, a state sponsor of terrorism, which provided financial backing, training, and operational guidance.

This partnership reveals how **organized crime syndicates enable terrorism**, offering access to illegal finance channels (like hawala), arms smuggling routes, and safe movement for operatives.

We discuss this nexus in detail in the later unit: **"Linkages with Internal Security: Crime-Terror Nexus."**

Student Notes:

3.1.5. India's Multi-Pronged Counter-Strategy to Terrorism

To combat this complex and evolving threat matrix, India has adopted a dynamic and multi-pronged counter-strategy that integrates diplomatic, legal, security, and financial measures.

Category	Measures
Diplomatic and Political Measures	
Isolating State Sponsors of Terrorism	- India has worked to **expose and isolate state sponsors of terrorism**, particularly Pakistan, at global forums like the UN. - Pakistan was placed on the FATF "grey list"  **FATF's Grip: Economic Pressure on Terror Financing** **FATF's grey-listing** (2018-2022) inflicted substantial economic pain on **Pakistan**, estimated at **$38 billion**. Under this international pressure, Pakistan notably convicted **Hafiz Saeed** on terror financing charges. Despite **China** providing a diplomatic shield, this case exemplifies how global **financial pressure** can compel states to act against **terrorist financing**. It underscores FATF's powerful role in international security.
Pushing for CCIT	- India advocates for the **Comprehensive Convention on International Terrorism (CCIT) at the UN to** criminalize all forms of international terrorism and cut off resources for terrorists.
Bilateral and Multilateral Security Cooperation	- Enhanced cooperation with like-minded countries via bilateral agreements and multilateral platforms like the **QUAD** and **SCO.** - The **RATS (Regional Anti-Terrorist Structure)** aims to promote better coordination among members of the Shanghai Cooperation Organisation (SCO) on **terrorism**.
Strengthening the Legal and Investigative Framework	
Strengthening Anti-Terror Laws	- Amendments to **UAPA (2019)** empower the government to **designate individuals as terrorists.** - NIA Act amendments enable NIA to investigate terror crimes outside India.
Empowering NIA	- National Investigation Agency (NIA) has become the premier agency for investigating terror crimes with interstate and international linkages.
Upgrading Security and Intelligence Architecture	
Enhancing Border Management	- Implementation of Comprehensive Integrated Border Management System (CIBMS), advanced technology to create a **"smart fence"**. - Fencing of the Indo-Myanmar border.

Student Notes:

Strengthening Intelligence Sharing	- Operationalization of **National Intelligence Grid (NATGRID)** for centralized security data. - Revamped Multi-Agency Centre (MAC) for real-time intelligence sharing.
Proactive Military and Security Doctrines	- Shift towards proactive security posture, demonstrated by Surgical Strikes (2016) and the Balakot Airstrike (2019) against terror infrastructure.
Countering Illicit Financial Flows	
Choking Terror Financing and Money Laundering	- Use of the Prevention of Money Laundering Act (PMLA) and stronger financial tracking to choke terror financing.
Role of FIU and NMFT	- Financial Intelligence Unit (FIU-IND) analyzes and disseminates financial intelligence. - Hosting the "No Money for Terror" (NMFT) Ministerial Conference to disrupt global terror financing networks. - A **Terror Funding and Fake Currency (TFFC) Cell** has been constituted in National Investigation Agency (NIA) to conduct focused investigation of terror funding and fake currency cases. **Cutting Terror Funds: Hawala to Crypto** India's **FIU-IND** actively combats **terror financing** via **Hawala crackdowns**, freezing significant funds (e.g., ₹1,200 cr scale in 2022-23) and initiating **PMLA cases**. However, **crypto-financing** presents a crucial, evolving **unregulated gap**. This highlights the continuous challenge of disrupting illicit financial flows for terrorism across new digital channels.

Operation Sindoor

Operation Sindoor, launched in **May 2025**, was a significant military campaign in response to the **Pahalgam terror attack**. This operation marked a pivotal shift in **India's national security strategy**, transitioning from a longstanding policy of **strategic restraint** to a more **assertive and proactive security posture**.

In this operation, Indian fighter jets used advanced **stand-off weapons**, launching their attack from within India's own territory.

Map Showing Targeted Sites in Pakistan and PoJK

- They relied on two main systems: the **SCALP**, a stealthy cruise missile designed to hit targets deep inside enemy lines, and the **HAMMER**, a jam-proof, all-weather precision bomb.
- The mission also involved **SkyStriker suicide drones**, each capable of carrying a 10kg warhead.

Student Notes:

Key Highlights:

- **End of Strategic Restraint**: Operation Sindoor signified the **end of India's policy of strategic restraint**, marking a shift to a more **assertive security approach**. This new approach clearly established "redlines," declaring **state-sponsored terrorism** as an **act of war** and **rejecting** the use of **nuclear blackmail**.
    - **Operation Sindoor showcased the Cold Start Doctrine in action**, with India launching **swift, precise conventional strikes inside Pakistan** in **response to terror attacks,** without triggering nuclear escalation.
- **Commitment to Decisive Retaliation**: The operation demonstrated India's readiness to take **decisive retaliatory action**, targeting **terror infrastructure** across **Pakistan**. The campaign included **military** and **non-kinetic actions** aimed at weakening terrorist networks.
    - In a recent statement, **India's National Security Advisor confirmed** that the military had **identified and struck 9 terror-related targets across the border,** successfully eliminating all without a single failure**.**
- **Imposing Tangible Costs on Pakistan**: The operation underscored India's commitment to imposing **tangible costs** on Pakistan for its role in sponsoring terrorism, reshaping **regional security dynamics**.
    - India launched precision strikes on **11 Pakistani airbases**—including **Nur Khan, Sargodha, Bholari,** and **Skardu**—and simultaneously destroyed major **terror infrastructure** across **Muzaffarabad, Kotli, Rawalakot**, and **Bagh**, including the demolition of **Masjid wa Markaz Taiba in Muridke** (LeT HQ) and **Jamia Masjid Subhan Allah in Bahawalpur** (JeM HQ)

Surgical Strike (2016)

A few years earlier, in **September, 2016**, the **Indian Army** carried out a **surgical strike** in direct response to a terrorist attack by **Pakistan-based militants** on an **Indian Army camp** in **Uri**, **Jammu & Kashmir**, on **September 18, 2016**, which resulted in the deaths of **19 Indian soldiers**.

- India launched a coordinated military operation across the **Line of Control (LoC)** into **Pakistan-occupied Kashmir**.
- Elite **Indian Special Forces** targeted multiple **terrorist launch pads**, where militants were preparing to infiltrate into Indian territory.
- The operation, called a "**surgical strike**" by the Indian government, was highly **precise**, **limited in scope**, and designed to avoid escalating the situation while showing India's ability to respond decisively against **cross-border terrorism**.

By publicly owning the operation, India shifted its defense stance from **strategic restraint** to a more **assertive approach** towards **Pakistan's use of terror groups** as proxies in **Kashmir**. The surgical strike sent a strong **political** and **military message** to Pakistan, signaling that India would act decisively to defend its sovereignty and would no longer tolerate **cross-border terrorism**.

Shifts and Updates in Internal Security Doctrine

India's New Security Doctrine (2025):

After **Operation Sindoor**, **Prime Minister Modi** outlined three key pillars:

Decisive Retaliation: Responding swiftly and forcefully to **terrorism**.

No Tolerance for Nuclear Blackmail: Rejecting nuclear threats to India's **self-defense** rights.

No Distinction between Terror Sponsors and Terrorists: Holding both **state sponsors** and **non-state actors** equally accountable.

Economic Measures:

The doctrine now incorporates **economic tools** to pressure terror sponsors without resorting to **kinetic escalation**.

Student Notes:

India's 5 Point Non-military Measure against Pakistan after Pahalgam Attack

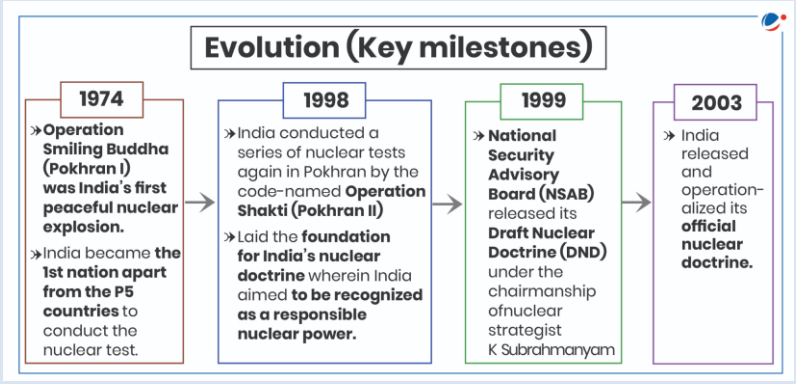
India's **national security strategy** has evolved sharply in response to cross-border terror attacks like the **Uri strike (2016)** and **Pulwama bombing (2019)**, both linked to **Pakistan-based groups** such as **Jaish-e-Mohammed (JeM)** and **Lashkar-e-Taiba (LeT)**. Post-2016 Uri Attack and 2019 Abrogation of Article 370

India's approach has become more **assertive**, with actions like the **surgical strikes** (2016), **Balakot Airstrikes (2019)** and **Operation Sindoor** (2025), marking a shift from **restraint** to **'deterrence by punishment'**, holding terrorists and their state sponsors directly accountable.

Unlike earlier responses, Operation Sindoor was followed by a **5-point non-military strategy**:

- **Suspension of the Indus Waters Treaty**: India has **suspended the 1960 Indus Waters Treaty** with Pakistan, halting river water sharing until Pakistan ends its support for cross-border terrorism.
- **Closure of Attari-Wagah Border Check Post**: India has **shut the Attari-Wagah border**, halting cross-border movement of people and goods, except for those with valid documents, who can return by May 1, 2025.
- **Cancellation of SAARC Visa Exemption Scheme (SVES)**: India has **revoked the SAARC Visa Exemption Scheme** for Pakistani nationals, canceling all issued visas and giving a 48-hour deadline for those in India to leave.
- **Expulsion of Pakistani Military Advisors**: India has **expelled all Pakistani military, naval, and air advisors** from the High Commission in New Delhi, with a reciprocal withdrawal of Indian military advisors from Islamabad.
- **Reduction of Diplomatic Personnel**: India will **reduce its diplomatic staff in Islamabad** to 30 by May 1, 2025, down from 55, further limiting bilateral engagement.

Together, these actions will ensure a **more comprehensive and lasting impact** of India's response.



India's Nuclear Doctrine and Operation Sindoor: Evolving Policies and Responses

India's **Nuclear Doctrine** is based on **Credible Minimum Deterrence (CMD)** and a commitment to **No First Use (NFU)**-meaning nuclear weapons will be used **only in retaliation** to a nuclear attack. In such a case, India promises **Massive Retaliation**, ensuring **Mutually Assured Destruction (MAD)** to deter first use by adversaries.

Do you know

As per, SIPRI Yearbook 2024, **India's arsenal increased from 164 in 2023 to 172,** representing a slight increase that has given it the two-warhead advantage over Pakistan.

It also pledges **non-use against non-nuclear weapon states**, reinforcing India's image as a **responsible nuclear power**. However, India reserves the right to respond with nuclear weapons in the event of **chemical or biological attacks**.

The doctrine is controlled by the **Nuclear Command Authority (NCA)**:

- The **Political Council**, chaired by the **Prime Minister**, authorises use.
- The **Executive Council**, led by the **NSA**, executes the order.

Following **recent terror attacks emanating from Pakistan(Uri till Pathankot)**, there have been **strong calls to review the doctrine**, especially the **NFU policy**. The turning point in this doctrine came with **Operation Sindoor**, where India launched swift conventional action **despite Pakistan's nuclear threats**.

Although the doctrine hasn't been officially updated, many analysts noted that **India "called off the nuclear bluff"** — challenging Pakistan's assumption that it could use **tactical nuclear threats** to **shield terrorism or proxy warfare**. Some commentators argued that Op Sindoor **effectively neutralised Pakistan's preemptive strike posture**, without breaching India's public nuclear stance.

4. Addressing India's Evolving and Interconnected Security Challenges

"Security is not a department; it is a culture." – K. Subrahmanyam

India's security challenges are multifaceted and interconnected, requiring a comprehensive and coordinated approach to safeguard its sovereignty and stability.

- **Addressing the Interconnected Nature of External Threats**
  - India's security challenges are deeply interconnected, involving **hostile state actors**, **violent non-state actors**, and **organized crime syndicates**.
  - **New domains** like **cyberspace** and **information warfare** amplify traditional threats, creating a complex security environment.
- **Adopting a Dynamic, "Whole-of-Government" Approach**
  - A **static** or **siloed** response is ineffective. India must implement a **dynamic** strategy, requiring **seamless coordination** among various agencies such as the **Home Affairs**, **Defence**, **External Affairs**, and **financial intelligence** agencies.
  - The approach should integrate **diplomatic**, **military**, and **internal security responses** to address evolving threats.
- **Building National Resilience**
  - Strengthening India from within is crucial. This involves **economic development**, **social cohesion**, and reinforcing **democratic institutions** to ensure all citizens feel secure.
  - A **strong**, **united**, and **prosperous India** is the best defense against external threats undermining its stability.

Israel's Integrated Security Model

The "**Whole-of-Government**" approach emphasizes integrated, collaborative security efforts. **Israel's National Security Council** exemplifies this as a **best practice model**, merging **Mossad, IDF, and cyber units**.

This seamless integration ensures comprehensive **coordination** across intelligence, military, and digital domains. It's crucial for swift, unified responses to complex national security challenges, demonstrating effective strategic synergy.

4.1. National Security Strategy: India's Urgent Need

An **NSS** is a **concise summary** of a country's **strategic vision** and **objectives**, encompassing both **domestic** and **external challenges**. It addresses **traditional** and **non-traditional threats** and **opportunities**, and is **updated periodically** to remain relevant to evolving security dynamics.

Student Notes:

Student Notes:

Why does India need a written National Security Strategy?

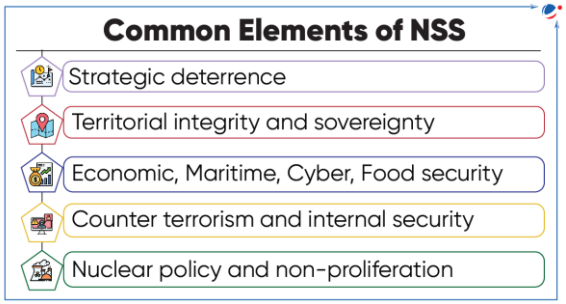
- **Lack of Written Policy & Continuity in Defence Planning**: India's **National Security Strategy** (NSS) relies on the **2009 Raksha Mantri's operational directive**, which remains outdated. The absence of **5-year** and **long-term defence plans** adds urgency to formalizing an updated, coherent **NSS** for strategic consistency.
- **Meet Changing Security Dynamics & Framework for Long-term Planning**: A **written NSS** would ensure regular reviews of **global security trends** and evolving threats like **hybrid warfare** and **Chinese naval growth**, fostering long-term **planning** while avoiding **short-term, ad-hoc** decisions on **national security** issues.
- **Strategic Signaling in World Order**: An **NSS** will clarify **India's strategic intent**, solidify its role as a **security provider** in the **Indian Ocean**, and strengthen **cooperation** with **international partners**, highlighting India's commitment to global security.
- **Operational Clarity & Reduce Ambiguity**: An **NSS** will provide **operational clarity** on key decisions such as **delegation** and **theatre command operationalization**, reducing **ambiguity** and enabling **accountability**, serving as a reference for **think tanks** to assess and refine security strategies.
- **Adopt Whole of Nation Approach**: A well-defined **NSS** will build **synergy** among national institutions, effectively coordinating operations to leverage **comprehensive national power** in addressing multi-dimensional security challenges.

Challenges in Codifying NSS in India

- **Lack of Political Will**: **Political consensus** on **national security issues** is lacking, and concerns over **accountability**, along with **limited expertise** on **defence matters**, have hindered the formulation of a formal **National Security Strategy** (NSS).
- **Loss of Strategic Flexibility**: Implementing an **NSS** would lock the **political leadership** into a specific approach, whereas **ad-hoc policymaking** allows **flexibility**, similar to how **Israel** operates without a formalized **NSS**.
- **Resource Allocation**: Effective implementation of the **NSS** requires adequate **financial resources**, **human resources**, and **capability-building** to meet its **objectives**, which has been a challenge in India.
- **Weak Institutional Support and Policy Feedback**: India has only a few **defence** and **security think-tanks**, leading to a lack of strong **institutional support** and **policy feedback**, which limits the effectiveness of the **National Security Strategy**

India's Previous Steps Taken to Draft NSS

- **The Kargil Review Committee Report (2000)**: It provided recommendations on **national security**, but did not lead to immediate **National Security Strategy (NSS)** formulation.
- **The Naresh Chandra Committee on Security (2011)**: Facilitated comprehensive **security reforms** discussions, but failed to drive the actual development of a formal **NSS**.
- **The Defence Planning Committee (2018)**: Chaired by the **National Security Advisor**, this permanent body is tasked with preparing a draft **National Security Strategy**.
- **Hooda Committee (2018)**: The **Hooda Committee** was formed to propose a comprehensive **National Security Strategy** to address evolving security challenges and enhance **India's defense capabilities**. It suggested tenets for the **draft NSS**, such as **global role**, **neighbourhood stability**, **internal peace**, **economic security**, and **strengthening capabilities** in **maritime borders**, **space**, and **strategic communications**.



Student Notes:

National Security Strategy (NSS) should outline clear **ends**, **ways**, and **means**, leveraging **delegation**, **synergy**, and **operational freedom**. It should encourage **initiative**, **innovation**, and **improvisation** at the **cutting-edge level**.

The Doval Doctrine: India's Assertive Security Paradigm

The **Doval Doctrine**, developed by **National Security Adviser Ajit Doval**, represents a shift from passive restraint to a **proactive**, **decisive**, and **pre-emptive** approach in India's security strategy. It emphasizes **national defense**, **counter-terrorism**, and **strategic deterrence**, based on Doval's experience in **counter-insurgency** and **intelligence**.

Key Tenets of the Doval Doctrine

- **Proactive National Defense**: India reserves the right to act offensively to neutralize threats, as seen in the **2016 surgical strikes** and **2019 Balakot airstrikes**.
- **Defensive-Offense Strategy**: A graduated response spectrum from **defensive** to **offensive**, signaling strong retaliation.
- **Zero Tolerance Towards Terrorism**: Terrorism and its **sponsors** are equally targeted, with an uncompromising response to all forms of **cross-border terrorism**.
- **Whole-of-Government Approach**: **Military**, **intelligence**, **police**, and **diplomatic** arms coordinate in a unified strategy.
- **Psychological and Informational Warfare**: Doval's doctrine includes **countering radical narratives** and waging **information wars**.
- **Security and Development Integration**: Combining **security operations** with **development initiatives**, particularly in **Kashmir** and **Left-Wing Extremism**.
- **No Compromise on Sovereignty**: India's sovereignty and **territorial integrity** are non-negotiable, particularly against **expansionist threats**.

Doctrine in Action

2016 Surgical Strikes & 2019 Balakot Airstrikes: Decisive actions in response to **cross-border terrorism**.

Abrogation of Article 370 (2019): **Integration** of **Jammu & Kashmir** using both **hard** and **soft power**.

Crackdown on Radical Groups: Operations against extremist **funding** and **support networks**.

China Standoff: **Forward deployment** and **muscular diplomacy** against **China's expansionism**.

Student Notes:

UNIT 3: CHALLENGES TO INTERNAL SECURITY THROUGH COMMUNICATION NETWORKS, BASICS OF CYBER SECURITY AND ROLE OF MEDIA AND SOCIAL NETWORKING SITES IN INTERNAL SECURITY CHALLENGES

"Cyberspace is the fifth domain of warfare, alongside land, sea, air, and space." – General Bipin Rawat, India's first Chief of Defence Staff

Previous Years Questions

Challenges to Internal Security through Communication Networks & Basics of Cyber Security

- **(2024)** Describe the context and salient features of the **Digital Personal Data Protection Act, 2023**. (10m, 150w)
- **(2022)** What are the different elements of **cyber security**? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy.(15 Marks)
- **(2021)** Keeping in view India's internal security, analyse the impact of **cross-border cyber attacks**. Also discuss defensive measures against these sophisticated attacks. (150 words)
- **(2020)** Discuss different types of **cyber crimes** and measures required to be taken to fight the menace.
- **(2019)** What is the **CyberDome Project**? Explain how it can be useful in controlling internet crimes in India.
- **(2018) Data security** has assumed significant importance in the digitized world due to rising cyber crimes. The Justice B. N. Srikrishna Committee Report addresses issues related to data security. What, in your view, are the strengths and weaknesses of the Report relating to the protection of personal data in cyberspace?
- **(2017)** Discuss the potential threats of **Cyber attack** and the security framework to prevent it.
- **(2015)** Considering the threats **cyberspace** poses for the country, India needs a "Digital Armed Force" to prevent crimes. Critically evaluate the National Cyber Security Policy, 2013 outlining the challenges perceived in its effective implementation.
- **(2015)** Discuss the advantage and security implications of **cloud hosting** of servers vis-a-vis in-house machine-based hosting for government businesses.
- **(2014)** What is **digital signature**? What does its authentication mean? Give various salient built-in features of a digital signature.
- **(2013) Cyber warfare** is considered by some defense analysts to be a larger threat than even Al Qaeda or terrorism. What do you understand about Cyber warfare? Outline the cyber threats which India is vulnerable to and bring out the state of the country's preparedness to deal with the same.

Role of Media and Social Networking Sites in Internal Security Challenges

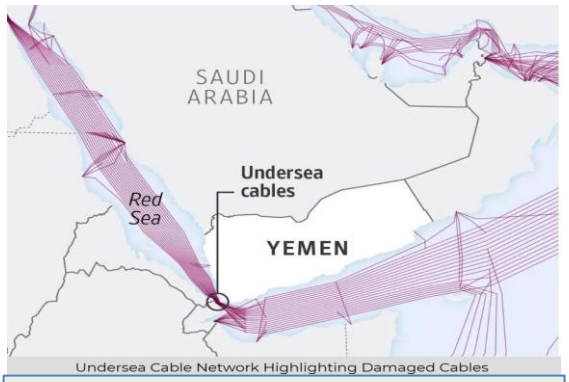
- **(2024) Social media** and **encrypting messaging services** pose a serious security challenge. What measures have been adopted at various levels to address the security implications of social media? Also suggest any other remedies to address the problem. (15m, 250w)
- **(2016)** Use of **Internet and social media** by non-state actors for subversive activities is a major concern. How have these been misused in the recent past? Suggest effective guidelines to curb the above threat.
- **(2015) Religious indoctrination** via **digital media** has resulted in Indian youth joining ISIS. What is ISIS and its mission? How can ISIS be dangerous for the internal security of our country?

- **(2013)** What are social networking sites and what **security implications** do these sites present?

Student Notes:

1. Communication Networks and Cyberspace

The **21st century** has introduced **cyberspace** and **communication networks** as critical domains of conflict, essential to **national security**. This digital ecosystem, comprising both physical and intangible infrastructure, has become a key driver of progress and a significant vector for internal security threats.



Undersea Cable Network Highlighting Damaged Cables

Undersea Cables: Global Internet's Fragile Lifelines

In **2024**, damage of **undersea cables** in the **Red Sea** disrupted **25% of data traffic** between Europe and Asia. This authentic incident exposed critical **vulnerabilities** in global internet infrastructure.

Such physical threats to vital communication networks pose a significant **cybersecurity challenge**. Protecting these **fragile lifelines** is crucial for maintaining global connectivity and economic stability.

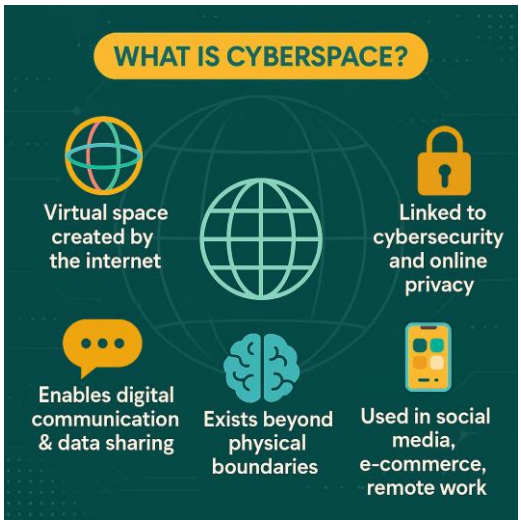
Communication Networks

Communication networks form the backbone of cyberspace, comprising both **tangible** and **intangible** infrastructure:

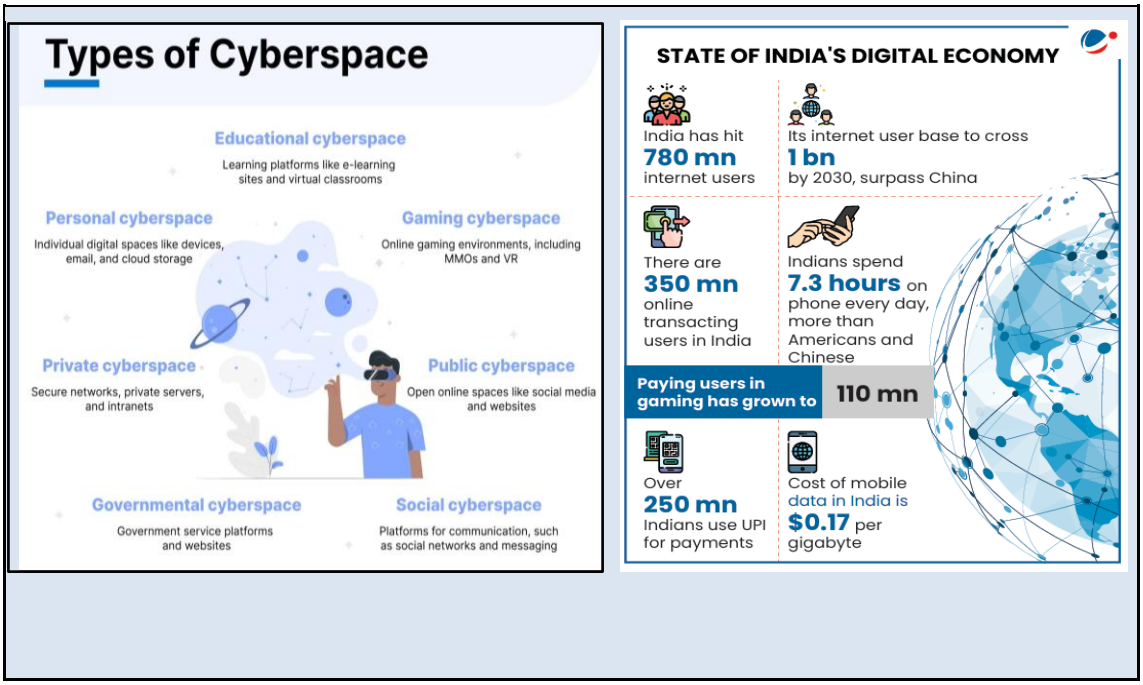
- **Physical Infrastructure**: Includes **optical fiber cables**, **undersea cables**, and **satellites** that connect global communication systems.
- **Wireless Infrastructure**: Covers **cellular networks** (from **2G to 5G**), **Wi-Fi**, and other **radio-based systems** facilitating wireless communication.
- **Hardware and Software**: Includes **routers**, **servers**, **mobile devices**, and the **protocols** governing their interactions.
- **Emerging Technologies**: The **Internet of Things (IoT)**, which links a vast network of **interconnected sensors** and **devices**.

Cyberspace

Defined by **India's National Cyber Security Policy (2013)**, **cyberspace** is described as a **"complex environment"** involving interactions between **people**, **software**, and **services** supported by global ICT networks.

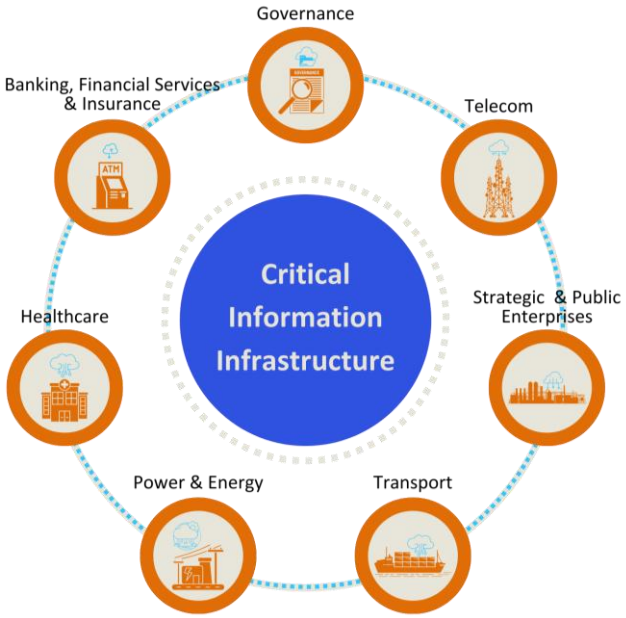


- Cyberspace is a **global** domain consisting of interconnected **networks**, **computer systems**, and **embedded processors**. Unlike traditional physical domains, cyberspace is **borderless**, **intangible**, and offers **anonymity** to actors, making it incredibly difficult to defend against malicious activities.
- This evolving digital landscape presents significant challenges to national security, requiring robust strategies to safeguard communication networks and cyberspace.



1.1. Criticality of Communication Networks for National Security

The increasing **integration of communication networks** into every aspect of modern life has made them essential for national functioning. As a result, these networks have become **high-value targets** for adversaries seeking to disrupt national security.



Networks as Critical Information Infrastructure (CII)

Under **Section 70** of **India's Information Technology (IT) Act, 2000**, certain **digital assets** are designated as **Critical Information Infrastructure (CII)**.

- **CII** is defined as **"computer resources, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health, or safety."**
- This official recognition highlights the paramount importance of securing these networks. Recently, the **IT resources of ICICI Bank**, **HDFC Bank**, and **NPCI** were declared as **CII**.

Interdependence of National Sectors and the "Cascading Effect"

Modern **critical sectors** such as **finance**, **energy**, **banking**, **transport**, **healthcare**, and **defence** are deeply interconnected and depend heavily on **communication networks**. A failure in one network can trigger a **"cascading effect"** across other sectors.

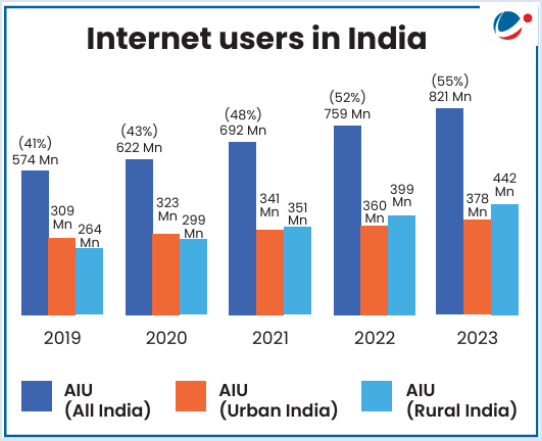
- For instance, a disruption in the communication network of the **power grid** could paralyze the **banking system**, **transportation networks**, and even **emergency services**, leading to widespread **chaos**.

Importance for National Initiatives and Associated Vulnerabilities

The success of major **government initiatives** like **Digital India**, **Smart Cities Mission**, and the **expansion of e-governance** is heavily reliant on a **stable and secure digital ecosystem**.

- India now has over **820 million active internet users**, including a large proportion in rural areas. While this drives **progress**, it also **vastly expands the attack surface**, increasing the vulnerability of both the **population** and **national infrastructure** to cyber threats.

The Current State of Cybersecurity in India



India is rapidly becoming a **digital society**, with over **820 million active internet users** today. More than half of these users, **442 million**, are from rural areas, and the total user base is projected to cross **1 billion by 2030**. While this massive growth, fueled by government programs like **Digital India**, drives progress, it also makes the country a prime target for cyber threats.

The scale of the problem is alarming. According to the **National Crime Records Bureau (NCRB)**, India saw a **24% rise in registered cybercrimes in 2022** compared to the previous year. The primary motive for these crimes is **fraud**, accounting for nearly 65% of all cases, followed by **extortion** (5.5%) and **sexual exploitation** (5.2%). Globally, a 2021 FBI report ranked India **third in the world** among the top 20 countries victimized by internet crimes. The intensity of these threats is also increasing, with the average Indian organization facing **2,807 cyber-attacks per week** in the first quarter of 2024—a 33% increase from the year before.

India has experienced several high-profile cyber-attacks that highlight its vulnerabilities:

- In 2012, a major breach compromised the email accounts of about **12,000 people**, including officials from the **Ministry of Home Affairs**, **DRDO**, and the **Indo-Tibetan Border Police (ITBP)**.
- In 2013, the **Nuclear Power Corporation of India (NPCIL)** reported that it had to block up to **ten targeted attacks per day**.
- In 2016, a massive data breach comprised **32 lakh debit cards** across the country.
- The hacker group **'Legion'** claimed to have accessed over 40,000 servers in India, including those of private hospital chains and some Indian banks.
- Food-tech company **Zomato** had the data of **17 million users stolen** and put up for sale on the dark web.
- The global **WannaCry ransomware attack** impacted thousands of computers in India, including systems belonging to the Andhra Pradesh police and utilities in West Bengal.
- The **Petya Ransomware attack** in 2017 disrupted container handling functions at a terminal in Mumbai's **Jawaharlal Nehru Port Trust**.

2. Threats in the Digital Domain: Cyber Warfare, Crime, and Terrorism

The **digital domain** has become a battleground where adversaries target the infrastructure that supports a nation's **economy** and **governance**. These **cyber threats**, which range from state-sponsored **cyber warfare** to financially motivated **cybercrime**, aim to **paralyze**, **disrupt**, and inflict **economic** and **strategic damage**.

Student Notes:

2.1. State-Sponsored Cyber Warfare and Espionage

Nations now use cyberspace as a primary tool of state power. Government-backed actors conduct aggressive attacks to disrupt infrastructure or carry out covert espionage to steal secrets, turning the digital world into a new battlefield for international conflict.

Stuxnet: Cyber Warfare Physical Impact

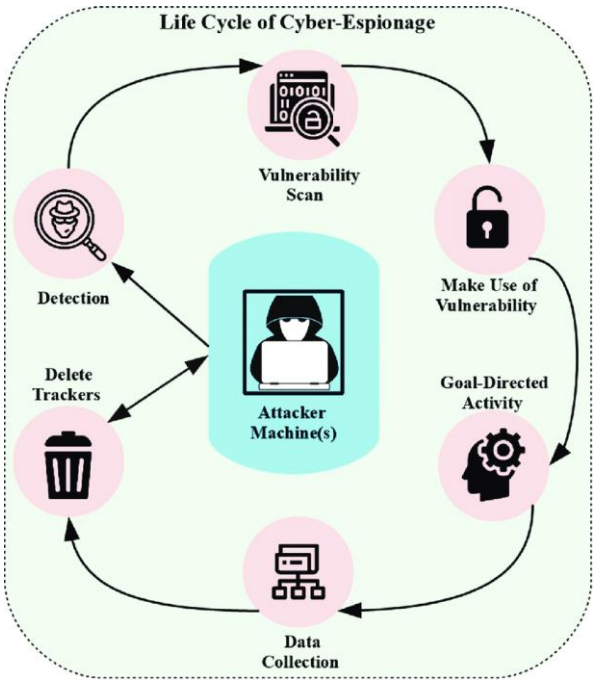
Stuxnet (2010), a **US-Israeli cyberweapon** (Operation Olympic Games), destroyed around **1,000 Iranian nuclear centrifuges**. This marked the first known cyber attack causing **physical destruction**.

It starkly demonstrated **Critical Information Infrastructure (CII)'s vulnerability** to **state-sponsored attacks**. This case cemented cyberspace as a new, potent **domain of warfare**, with real-world consequences.

2.1.1. Cyber Warfare: State-Sponsored Digital Assaults

Cyber warfare is the use of **computer technology** by a state to disrupt the activities of another state, typically by attacking **information systems** for **strategic or military purposes**.

- **Objective**: Disable or destroy an adversary's **critical infrastructure**, such as **power grids**, **financial systems**, and **military networks**.
- **Case Study (International)**: The **Stuxnet worm** was a sophisticated, state-sponsored malware designed to damage Iran's nuclear centrifuges by manipulating their **industrial control systems**.
- **Indian Context (Operation Sindoor, May 2025):** The conflict following Operation Sindoor marked the first time cyberspace became an active and coordinated theatre of war between India and Pakistan. Pakistani threat actors, often with support from China, launched a massive wave of attacks to create a "fog of war", including:
- **Distributed Denial of Service (DDoS) Attacks:** A spike in DDoS attacks targeted at least 15 major Indian government organizations, including the Income Tax Department, Hindustan Aeronautics Limited (HAL), and Indian Railways.
    - A report by Maharashtra Cyber recorded over **1.5 million cyberattacks** during the crisis period.



- **Malware Deployment:** A prominent Pakistani group, **APT-36** (also known as Transparent Tribe), deployed malware like the **Crimson Remote Access Trojan (RAT)** to target Indian government and defence personnel and harvest sensitive information.
- **Website Defacements:** A familiar tactic was the defacement of Indian websites, including that of the **Armoured Vehicle Nigam Ltd**, a defence public sector unit.

2.1.2. Cyber Espionage: Covert Theft of Sensitive Data

Cyber espionage involves the **illicit access** of confidential information through computer networks, aimed at stealing **strategic, military, or economic secrets**.

Student Notes:

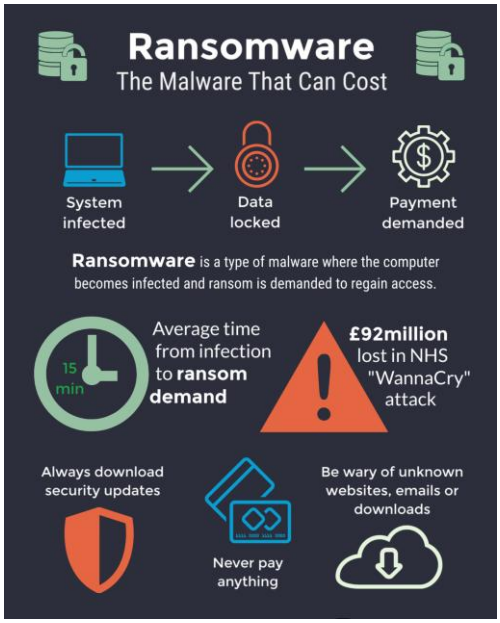
- **Case Study (International)**: The **NSA surveillance program**, revealed by **Edward Snowden**, exposed large-scale data collection and espionage globally, including against India.
- **Case Study (China)**: The **Zhenhua Data leak** revealed a Chinese company linked to its government, collecting vast personal data on foreign leaders, military figures, and influential individuals, highlighting **digital espionage** for **"threat intelligence"**.

2.2. Cybercrime: Attacks for Disruption and Financial Gain

Cybercrime encompasses a wide range of illegal activities conducted over digital platforms. These attacks exploit vulnerabilities in systems and human behavior—affecting individuals, businesses, and government infrastructure—all with the intent of financial gain, data theft, or geopolitical disruption.

2.2.1. Extortion-Based Attacks: Coercion for Profit

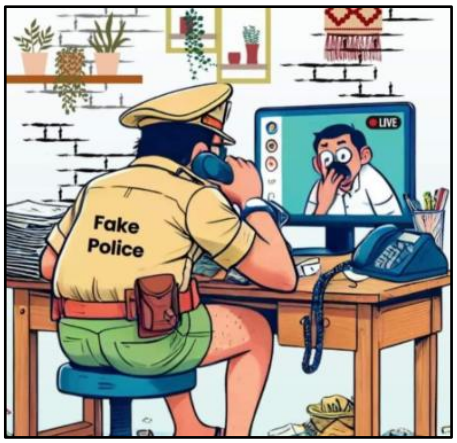
These sophisticated crimes use intimidation and digital lockdowns to force victims to pay money, representing a severe and growing threat.



- **Ransomware Attacks:** Ransomware remains one of the most damaging forms of cyber extortion. In these attacks, **malware encrypts key files and systems**, demanding payment—usually in **cryptocurrencies**—for access to be restored.

India saw a record **69% surge in ransomware attacks** between 2022 and 2023. Cyber threat reports also note **healthcare and public infrastructure sectors as prime targets** due to their lack of real-time backup systems.

- **Case Study: AIIMS New Delhi Ransomware Attack (2022)** India's premier medical institute, AIIMS, suffered a **crippling ransomware attack in November 2022**. The attack paralyzed its patient registration, diagnostic, billing, and eHospital systems for over two weeks. The attackers, suspected to be Chinese-origin cybercriminals, demanded **nearly ₹200 crore in cryptocurrency** and leaked patient data online.
- **Digital Arrest Scams:** A rising form of **social engineering cybercrime**, **digital arrest scams** saw a dramatic increase in 2024. Criminals **impersonate law enforcement agencies** like the **CBI or cybercrime branch**, using **fabricated arrest warrants** and fake documentation to threaten victims.



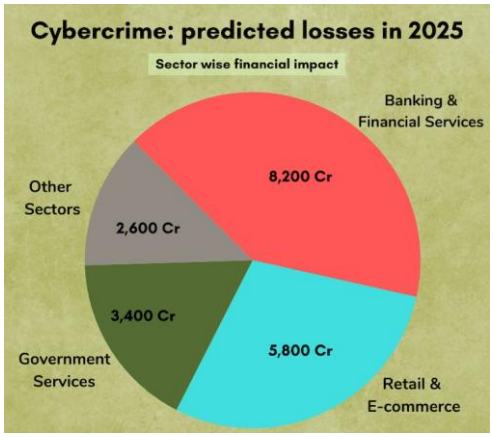
The scam's success relies on a combination of **psychological manipulation** (using fear and authority) and **digital.** Victims are coerced into "digital house arrest" by staying on continuous video calls and paying hefty "bail" amounts.

- In just **three months** of 2024, over **₹120 crore** was lost due to these scams. In many cases, **foreign-based call centers and WhatsApp numbers** were traced as the source of the crime.

Student Notes:

2.2.2. Theft and Fraud-Based Attacks: Stealing Data and Money

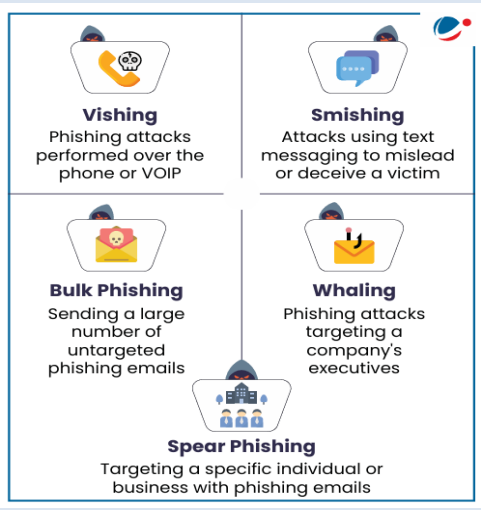
These attacks are focused on illicitly acquiring funds or valuable personal information through technical breaches and deception.



- **Hacking Financial Systems & Accounts** There has been a flagged rise in **unauthorized remote access fraud**, with criminals taking control of desktops via fake customer support links (e.g., **AnyDesk scams**). A major scam in February 2024 breached **YES Bank's UPI services**, affecting over **12,000 users** with estimated losses exceeding **₹10 crore**.
- **Credit/Debit Card Data Theft Card cloning and skimming scams** have become the most reported online financial fraud, making up **42% of all cyber complaints**. Leaked datasets with millions of Indian card details were found on the **dark web in May 2025**, traced to breaches in payment gateway plugins.
- **Phishing Attacks** Phishing continues to be a primary technique for credential theft in India. A recent mass phishing campaign impersonated the **Income Tax Department**, targeting **PAN and Aadhaar** holders by offering fake refunds. In April 2025, cyber police in Hyderabad busted a ring stealing **KYC data from over 1.6 lakh Indians** and selling it online.

Main Cyber Players and Their Motives

- **Cyber Criminals**: Seeking **commercial gain** from hacking **banks** and **financial institutions**, as well as **phishing scams** and **computer ransomware**.
  - **Phishing** is a broad term for **cyberattacks** that use **social engineering** to trick victims into paying money, handing over **sensitive information**, or downloading **malware**.
- **Cyber Terrorists**: With the mission to penetrate and attack **critical assets** and **national infrastructure** for aims relating to **political power** and **"branding"**.
- **Cyber Hacktivists**: Groups such as "**Anonymous**" with **political agendas** that hack sites and servers to virally communicate the **"message"** for specific campaigns.



2.3. Cyber Terrorism: The Digital Front of Fear

Cyber terrorism is the **politically or ideologically motivated use of technology** to carry out disruptive attacks against computer systems and networks. The primary goal is not financial gain, but to **instill fear, cause widespread harm, or intimidate a society** to achieve a political objective. It represents a modern form of terrorism where the battlefield is digital, but the consequences can be devastatingly real.

- **Objective:** To **destabilize society** by attacking critical national infrastructure, **generate widespread fear** through high-profile disruptions, and **advance a political, religious, or ideological agenda** by causing severe economic damage or even loss of life.
- **Primary Methods:**
  - **Disruptive Attacks:** Crippling essential services using **Distributed Denial of Service (DDoS)** attacks. During **Operation Sindoor (May 2025)**, over **1.5 million DDoS attacks**

were recorded against Indian digital infrastructure, targeting the **Income Tax Portal, Indian Railways**, and **HAL**. Botnets traced to **Pakistani and Chinese locations** were linked to these attacks.
    - **Infrastructure Sabotage:** Introducing malicious software like the **Stuxnet worm** to damage physical systems, such as power grids or industrial controls. Malware families such as **Emotet, Lokibot**, and **Crimson RAT** (used by Pakistan-based **APT-36/Transparent Tribe**) are actively used to target India's strategic sectors mainly affecting small and medium enterprises (SMEs) and educational institutions
    - **Hacking and Data Breaches:** Infiltrating government or military networks to steal, alter, or destroy sensitive data.
- **Common Targets:**
    - **Critical National Infrastructure:** Power grids, water supply systems, transportation networks, and hospitals.
    - **Government & Financial Systems:** Military command networks, emergency services, and banking institutions.
    - **Public Information Platforms:** Media outlets, which can be manipulated to spread propaganda and misinformation.
- **The Key Distinction from Cybercrime:** What separates cyber terrorism from standard cybercrime is **motivation**. While cybercriminals seek **financial gain**, cyberterrorists aim for **political or ideological impact**. An attack to steal credit card data is cybercrime; an attack to shut down a nation's power grid to cause panic is cyber terrorism.
- **Global Context & Challenges:** There is currently **no universal legal definition** of cyberterrorism, making international cooperation complex. Meanwhile, the threat grows as attacks become more sophisticated and anonymous, with both **non-state groups and clandestine state agents** leveraging technology for terror.

3. The Evolving Threat Matrix: The Next Generation of Challenges

3.1. The Security Implications of 5G Technology

"Who controls 5G controls the battlefield."– NATO Cyber Defence Report, 2023

The **rollout of 5G technology**, which promises ultra-low latency and enhanced connectivity, introduces new **security vulnerabilities** that could compromise both infrastructure and national security.

Increased Attack Surface and Supply Chain Vulnerabilities

- **Increased Attack Vectors**: With the connection of billions of devices under the **Internet of Things (IoT)**, from **smart cities** to **industrial control systems**, 5G significantly expands the attack surface. This creates far more entry points for potential cyber attackers than 4G networks.
- **Software-Defined Networking**: Unlike previous generations that relied on **centralized hardware**, 5G networks are **software-defined** and **virtualized**, meaning an attacker controlling the software could potentially seize control of the entire network.
- **Supply Chain Risks**: A major concern is the reliance on foreign vendors for **5G equipment**. Hardware from companies with potential links to foreign governments may contain **embedded malware**, **spyware**, or **backdoors** that could be exploited for **espionage** or to **disrupt networks** in times of crisis.

3.2. Artificial Intelligence (AI) as a Dual-Use Technology

AI is a **transformative technology** that serves both **defenders** and **attackers**, significantly altering the landscape of **cybersecurity**.

Student Notes:

Student Notes:

1. **AI-Powered Malware and Automated Cyber-Attacks**
   - **AI-powered malware** is evolving to become **smarter**, learning, adapting, and altering its code to evade detection by traditional antivirus systems.
   - **Automated cyber-attacks**: AI enables large-scale **automated attacks** that can find vulnerabilities and exploit them without human intervention, creating a much more dangerous and effective form of cyber warfare.

2. **Deepfakes for Disinformation**

   Deepfakes, highly realistic **AI-generated videos** or **audio clips**, can make it appear as though individuals have said or done things they never did.

   - **Impact**: Deepfakes can be used for **disinformation**, **propaganda**, and **defamation**, posing serious threats to **social stability** by misleading the public and inciting unrest or violence.

Deepfakes in Warfare: Zelenskyy's Test

During the Ukraine War, a **deepfake video** of **Zelenskyy "surrendering"** circulated (notably 2022).

Its aim was to **demoralize troops**.

This highlights **AI's weaponization** for **information warfare**. It shows how manipulated media can significantly impact morale and security.

3. **Hybrid and Grey-Zone Warfare**

   Hybrid warfare blends conventional and unconventional tools, including **cyberattacks**, **information operations**, and **economic coercion**, to achieve strategic goals without formal military conflict.

   Understanding Hybrid Warfare

   - **Hybrid Warfare** combines **kinetic** and **non-kinetic** tools, operating in the **"Grey Zone"**, a space between peace and full-scale war. It allows adversaries to act ambiguously and deniably.

Asymmetric Warfare: Strategies of Unequal Combat

Asymmetric warfare is a conflict between two sides with very unequal military power. Instead of fighting a conventional battle they would likely lose, the weaker side uses clever and **unconventional tactics**.

These methods include **guerrilla warfare, cyberattacks, terrorism, sabotage**, and **proxy warfare**. The goal isn't to win a head-on fight, but to inflict damage and cause disruption through speed and surprise.

This type of conflict is often seen between a nation's regular army and **non-state actors**. Key examples include the war in **Ukraine** (against Russia), the conflict in **Yemen** (**Houthi Rebels vs. Saudi-led Coalition),** and the **Israel-Palestine conflict** involving groups like **Hamas**.

   - **Example**: Israeli and **Iranian hybrid** tactics involve **aerospace strikes**, **cyber operations**, **assassinations**, and **drone warfare** to target critical infrastructure. Both nations use **proxy mobilization**, **psychological operations**, and **disinformation** to exert influence, relying on **asymmetric** strategies for covert, deniable attacks.

4. Building Digital Resilience - India's Counter-Strategy

The **digital domain** is increasingly being weaponized by **state** and **non-state actors** to wage a new form of warfare. This conflict not only targets physical infrastructure but also seeks to undermine **social cohesion** and **governance**. At the heart of this warfare is **Information Warfare**, with the objective of controlling narratives, manipulating public opinion, and sowing discord.

This evolving threat necessitates a **multi-layered approach** to safeguard its critical infrastructure, counter cyber threats, and promote national security in cyberspace. Key aspects of building Digital Resilience for India are:

Student Notes:

4.1. Legal and Policy Framework

- **The Information Technology (IT) Act, 2000 and Amendments:** The **IT Act, 2000** is India's primary legislation for **cybercrime** and **electronic commerce**.
  - Amendments have strengthened the focus on cybersecurity, criminalizing **identity theft**, **phishing**, and **cyber terrorism** . It provides the legal basis for actions such as blocking websites and online content threatening **national security**.
- **The Digital Personal Data Protection Act, 2023:** Enacted to address **data security**, this Act ensures **individuals' rights** and **data fiduciaries' obligations** regarding the protection of personal data.
  - It establishes a **Data Protection Board of India** to handle grievances, ensuring accountability and minimizing data misuse.
- **National Cyber Security Policy (NCSP), 2013:** India's first dedicated policy aimed at creating a secure cyberspace. It set ambitious goals, including the training of **500,000 cybersecurity professionals**. However, challenges such as a **shortage of skilled manpower** remain, necessitating updates to the policy.
- **The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:** These rules regulate **social media intermediaries**, requiring them to appoint **grievance officers**, identify the **first originator** of harmful content, and remove content flagged by authorities.

INDIA AND THE BUDAPEST CONVENTION

Budapest Convention-International Cybercrime Framework

The **Budapest Convention** is the first **legally binding international treaty** on **cybercrime**, aiming to harmonize national laws on offenses like **hacking** and **fraud**, improve investigative techniques, and foster **international cooperation** for collecting **electronic evidence**.

India declined to sign the **Budapest Convention** due to concerns over **sovereignty** and **data access** provisions. Instead, India advocated for a new **UN Cybercrime Convention**, which was adopted in **2024** and will open for signature in **2025**.

Bharat NCX 2024-Boosting Cyber Defenses

CERT-In's Bharat NCX 2024, India's largest **cyber drill**, simulated 2,000 attacks on vital **banking** and **power grids**. It successfully trained 150 agencies, significantly enhancing India's **cybersecurity** preparedness against complex threat.

4.2. Institutional Architecture

- **CERT-In (Indian Computer Emergency Response Team)**: The **national nodal agency** responsible for **responding to cybersecurity incidents**, issuing advisories, and coordinating the national response to cyber threats.
- **National Cybersecurity Coordination Centre (NCCC)**: A cyberspace intelligence agency focused on **security** and **electronic surveillance**. It screens **communications metadata** to detect real-time **cyber threats** and coordinates with law enforcement for **intelligence gathering**.
- **NCIIPC (National Critical Information Infrastructure Protection Centre)**: Mandated to protect **critical infrastructure** from cyber threats, NCIIPC ensures the security of key sectors like **energy, banking, and healthcare**.
- **I4C (Indian Cyber Crime Coordination Centre)**: Operates under the **Ministry of Home Affairs** and provides a platform for citizens to report cybercrimes, ensuring better coordination between law enforcement agencies.
- **Role of NSCS and NCSC**: The **National Security Council Secretariat (NSCS)** and **National Cyber Security Coordinator (NCSC)** play a key role in coordinating national strategies and advising the **Prime Minister's Office** on security matters.

Student Notes:

National Cybersecurity Coordinator (NCSC)

The **National Cybersecurity Coordinator (NCSC)** was created under the **National Security Council Secretariat (NSCS)** to coordinate national **cybersecurity efforts**. It aligns the efforts of **central agencies**, **state governments**, and **international bodies** to secure India's digital infrastructure. The NCSC is responsible for advising the **Prime Minister's Office (PMO)** on **cyber threats** and **policy**.

Functions and Responsibilities: NCSC leads a **whole-of-government approach**, coordinating **cybersecurity policies** across ministries and sectors. It provides **strategic direction** and monitors **cyber threat** detection, **response** efforts, and **cybercrime investigations**. It collaborates with **CERT-In**, **NCIIPC**, and **sectoral regulators** like **RBI** and **TRAI** to enhance national cybersecurity resilience.

Leadership: Lt. Gen. M U Nair assumed the role of **NCSC** in **2023**, bringing expertise in **cyber warfare**, **signal intelligence**, and **communication technologies**.

Key Challenges: NCSC faces challenges in maintaining **cybersecurity preparedness** amidst an evolving cyber threat landscape. Strengthening its **response capacity**, ensuring **inter-agency cooperation**, and increasing **international collaboration** are key areas of focus to overcome these challenges. The NCSC is essential for India's long-term **cyber resilience** and **defense**.

4.3. Other Key Initiatives and Doctrines

- **Cyber Swachhta Kendra**: A government initiative providing **free tools** to citizens to detect and **remove malware and botnets**, promoting **digital hygiene**.
- **Cooperation with Other Countries**: India collaborates with countries like the **UK**, **USA**, **China**, and **Singapore** on **cybersecurity training**, **information exchange**, and **joint combat against cybercrime**.
- **State Government Initiatives**:
  - **Telangana**: First state with a **cybersecurity policy** and **Cybersecurity Center of Excellence**.
  - **Kerala**: **Cyberdome** for police training in combating emerging cyber threats.
  - **Maharashtra**: **Cyber Safe Women** initiative to raise awareness on **cyber safety**.

CyberDome: Collaborative Security

Kerala's CyberDome is a **best practice PPP initiative**. It effectively links **police, ethical hackers, and academia** to bolster **cybersecurity**.

Its focus on **threat intelligence** and **drills** helps protect **Critical Information Infrastructure (CII)**. This collaborative model is crucial for robust cyber defense.

- **Audit of Government Websites**: Empaneling organizations to audit and implement **information security best practices**.
- **Digital Armed Force**: There is growing discourse on establishing a **dedicated Cyber Command** with both **defensive** and **offensive** capabilities to protect India's **cyber interests**.

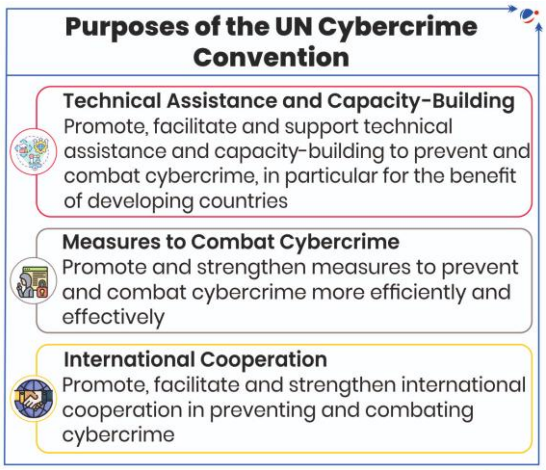
4.4. United Nations Convention on Cybercrime

The **UN Cybercrime Convention** is the first legally binding UN instrument on cybercrime, adopted by 193 member states. It focuses on **preventing, investigating**, and **prosecuting cybercrimes**, and ensures **electronic evidence sharing**. It will be signed in 2025, effective after 40 states join.

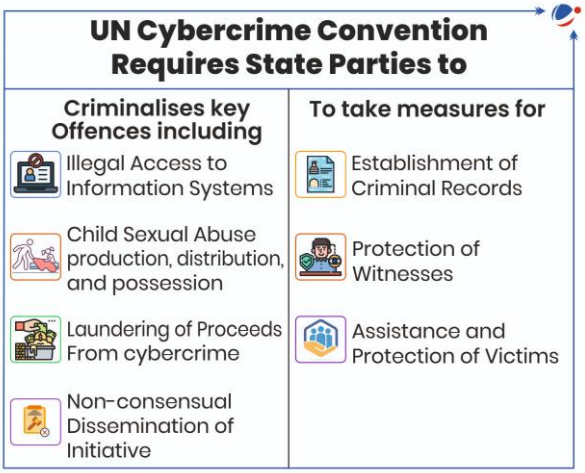
Key Provisions of the Convention

- **International Cooperation & Data Sharing**: Facilitates mutual legal assistance, extradition, and a 24/7 network for urgent cooperation.

- **Procedural Measures**: Provides guidelines for law enforcement on preserving, searching, and seizing electronic data.
- **Protection of Personal Data**: Ensures compliance with privacy laws and encourages bilateral agreements for data sharing.
- **Protection of Human Rights**: Safeguards human rights and freedoms during the implementation of cybercrime procedures.
- **Other Provisions**: Covers extradition, transfer of sentenced persons, criminal proceedings, and joint investigations.



The **Convention** addresses the growing risks of **cybercrime** due to increased **connectivity**, especially in **Southeast Asia**. It promotes **global cooperation**, rapid **evidence-sharing**, and adaptation to **technological advancements**. It also ensures **child protection** and rehabilitates **victims of cybercrimes**.

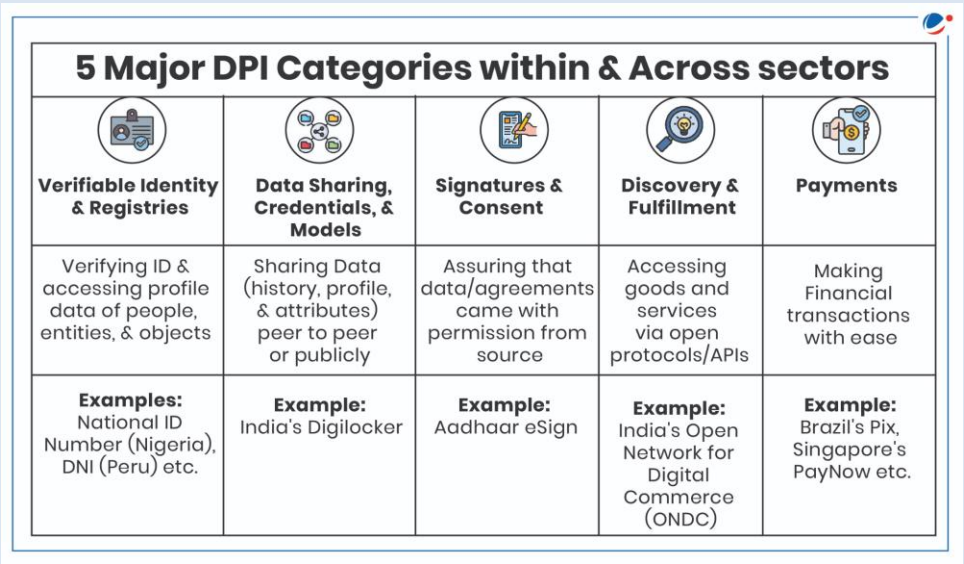


Digital Public Infrastructure

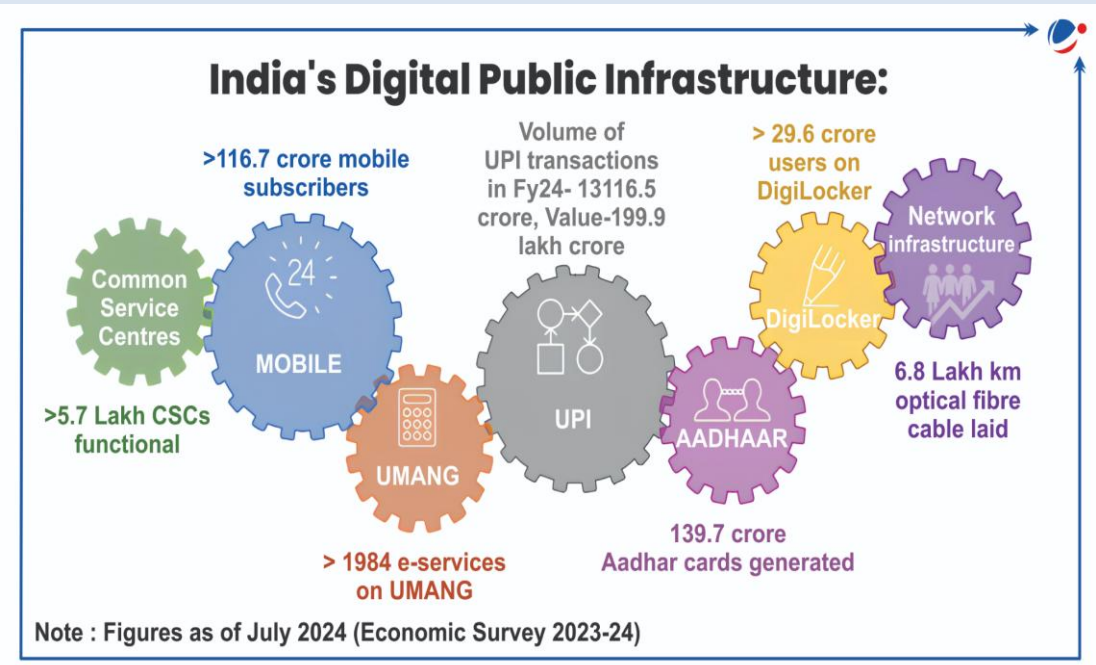
Digital Public Infrastructure (DPI) comprises **shared digital systems** like **identity, payments, and data exchange**, built on **open standards**. These foundational "digital rails" enable efficient, inclusive delivery of essential **public and private services** at a societal scale.

India's DPI, including **Aadhaar, UPI, and CoWIN**, is projected to be a **$1 trillion economic asset** by 2030. This makes it a powerful **geopolitical tool** for global expansion.

However, its international spread introduces substantial **cyber-espionage risks**, making its **integrity and robust cybersecurity paramount** against malicious actors.



Student Notes:



Challenges in Building Resilient Digital Infrastructure

- **Dependence on Imported Hardware and Software**: India's reliance on **imported telecom hardware** exposes it to **supply chain vulnerabilities**, highlighting the need for **self-reliance** in **5G technology** and **domestic manufacturing**.
- **Shortage of Cybersecurity Workforce**: Despite the **National Cyber Security Policy (2013)**, India faces a **shortage of cybersecurity professionals**, requiring greater **training** and **capacity building** to meet goals.
- **Balancing Security and Privacy**: India struggles with the balance between **national security** and **citizen privacy rights**, particularly concerning **end-to-end encryption** and **law enforcement** efforts.
- **Inter-agency Coordination**: Fragmented **central-state coordination** creates gaps in **information sharing**, with India's **federal structure** complicating **cybersecurity** implementation across jurisdictions.

Recommendations for Building Resilient Digital Infrastructure

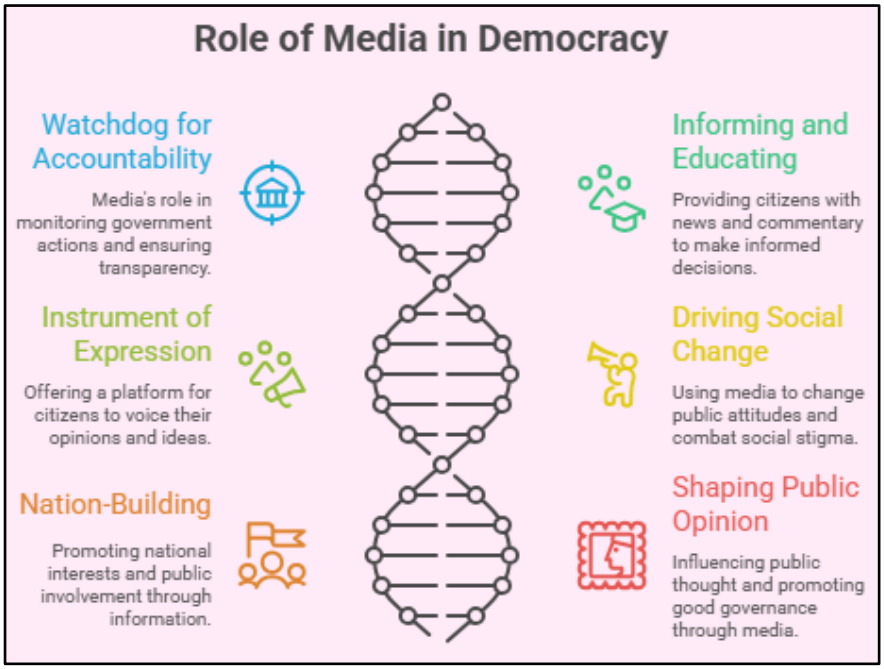
- **Building Indigenous Capabilities ('Aatmanirbhar' in Cyberspace)**: India must focus on **domestic manufacturing** and **R&D** in **telecom hardware** and **cybersecurity solutions**, ensuring **self-sufficiency** and enhanced security.
- **Strengthening International Cooperation**: India must enhance **international collaboration**, focusing on **real-time intelligence sharing** and **joint cyber investigations** to counter **transnational cyber threats** effectively.
- **Public-Private Partnerships (PPP)**: Strong **public-private partnerships** like **CyberDome** in **Kerala** will boost **CII protection** and **cybersecurity efforts**, improving **state-level cooperation** for defense.
- **Promoting Cyber Hygiene and Public Awareness**: A **national awareness campaign** focusing on **strong passwords**, **multi-factor authentication**, and **phishing prevention** will help create a **cyber-resilient society**.

Student Notes:

5. Role of Media and Social Networking Sites in Internal Security Challenges

India's **media ecosystem** is diverse and multifaceted, comprising various types that cater to its vast and multilingual population. The main kinds of media in India include:

- **Print Media**: Traditional **newspapers** and **magazines** published in multiple languages remain influential sources of **news**, **opinions**, and **entertainment**.
- **Broadcast Media**:
  - **Television**: Includes public broadcaster **Doordarshan** and multiple **private channels** offering news, entertainment, regional content, and satellite services.
  - **Radio**: Both public (**AIR - All India Radio**) and private **FM stations** broadcast news, music, and cultural programming.
- **Over-The-Top (OTT) Media Services**: Streaming platforms delivering **video-on-demand** over the internet. India hosts about 57 **OTT providers**, such as **Amazon Prime Video**, **Netflix**, **JioCinema**, **Disney+ Hotstar**, **ZEE5**, **SonyLIV**, and regional platforms like **Aha (Telugu)**, **Planet Marathi**, and more, offering content in numerous regional languages.



- **Digital and Social Media**: Rapidly growing platforms essential for **communication**, **news dissemination**, and **entertainment**. Key **social media platforms** widely used across India include:
  - **WhatsApp**: Leading **instant messaging app** with over 400 million users.
  - **Facebook**: Over 320 million users, serving as a broad **social networking site**.
  - **Instagram**: Popular among youth for **photo** and **video sharing**, with around 230 million users.
  - **YouTube**: A top **video-sharing platform** hosting diverse content tuned to Indian audiences.

5.1. Internal Security Threats from Broadcast and Print Media

Both television channels (broadcast media) and newspapers (print media) can pose serious threats to India's internal security. Based on past events and legal observations, these threats can be categorized as follows:

1. **Revealing Sensitive Operational Details**

   Live, minute-by-minute reporting of military or anti-terror operations is one of the most direct threats to national security.

Student Notes:

- During the **26/11 Mumbai terror attack**, the **Supreme Court** heavily criticized TV channels for their live coverage. By showing the real-time movements of security forces, the media was essentially providing a playbook to the terrorists' handlers, putting the lives of both security personnel and citizens in jeopardy.
- Similarly, during the **military mobilisation in December 2001**, the media's detailed reporting on troop movements was so extensive that it was compared to doing the spying job for Pakistan's intelligence agency, the **ISI**.

2. Fueling Communal and Social Unrest

The media can act as a catalyst for social instability and communal violence through irresponsible reporting and the spread of unverified news.

- **Sensationalism and Fake News:** The relentless competition for "Breaking News" often leads to channels airing unverified information that can cause widespread panic. A key example is the **2016 Kairana "exodus"** story, where false claims of Hindu families fleeing a Muslim-majority town were amplified by certain media outlets, leading to severe **communal polarization**.
- **Targeted Narratives and "Information Warfare":** The media can become a tool in **information warfare** when it broadcasts inflammatory content that makes a **religious minority** a target or harms a community's dignity. Furthermore, the trend of conducting **"Media Trials"** creates a form of "tele-terror" or **"digital violence"** that can destroy reputations and incite public anger, interfering with the legal process long before a court has delivered a verdict.

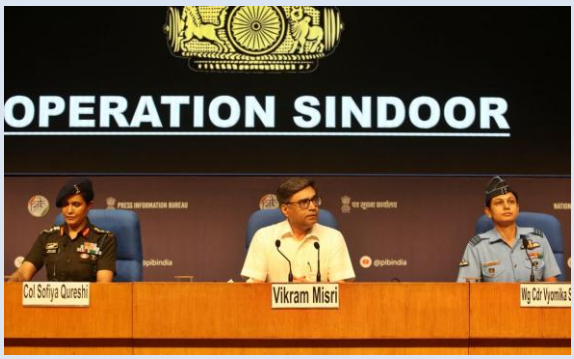
3. Platforming Divisive and Secessionist Forces

The media becomes a direct threat when it gives a platform to individuals or groups that aim to harm the country's unity. By providing airtime and print space to **secessionist groups**, the media can unintentionally legitimize their cause and help them broadcast their divisive ideologies to a wider audience, thereby threatening the **integrity of the nation**.

4. Misrepresenting Critical Security Issues

The media can be irresponsible when it politicizes or oversimplifies complex national security challenges. For example, in its coverage of the long-running **Pakistani Proxy War in Jammu & Kashmir**, the media has, at times, ignored India's **"strategic sensitivities"**. By focusing heavily on themes like **Kashmiri alienation** without a balanced perspective, it can create a distorted understanding of the conflict and weaken the national resolve.

Indian TV Media and Operation Sindoor: A Tale of Two Narratives



During **Operation Sindoor**, the Indian public received information from two very different sources: fast-paced private news channels and disciplined official government channels, each telling the story in its own distinct way.

Private News Channels: Sensationalism and 24/7 Coverage

Private networks like **Aaj Tak**, **News18**, and **India Today** provided round-the-clock coverage defined by a high-energy, breaking-news culture.

- **Reporting Style:** Their reporting often prioritized speed over verification, leading to **sensationalism**. This included airing unconfirmed reports and speculative military analysis.

- **Studio Debates:** Their dramatic studio debates, often accused of **war-mongering** and of discussing strategy and the risks of nuclear escalation, blurred the lines between information and entertainment.
- **Security Concerns:** A major issue was the **broadcasting** of **live footage** from **sensitive areas**, which risked revealing tactical information and could have compromised operational secrecy.
- **Countering Misinformation:** The fact-checking of Pakistani propaganda was inconsistent. While some channels worked to debunk rumors, others inadvertently spread them through uncritical reporting.

Official Channels: A Message of Control and Clarity

Government channels, led by **Doordarshan (DD) News** and official briefings from the **Ministry of Defence** and **Ministry of External Affairs**, adopted a highly disciplined and fact-driven approach.

- **Authoritative Updates:** Information was disseminated through carefully worded, centralized press briefings from senior military and government officials.
- **Consistent Messaging:** The official narrative consistently emphasized that **Operation Sindoor** was a **calibrated response** targeting only **terror infrastructure**, not civilians, in order to minimize escalation.
- **Countering Propaganda:** Senior officials, including **National Security Adviser (NSA) Ajit Doval**, directly countered false narratives from Pakistan with on-record denials. They also criticized some media outlets for amplifying speculation and urged the public to rely on verified official updates.

The two approaches had very different effects. **Private media** drove high public engagement and national debate but also risked stoking **public anxiety** and compromising **operational security**. In contrast, **official channels** focused on maintaining a **unified national message**, promoting calm, and ensuring information security.

5.2. The Evolving Threat of Social Media to India's Internal Security

In recent years, social media platforms like **Facebook**, **Twitter**, **WhatsApp**, and **YouTube** have transformed from simple communication tools into major vectors for internal security threats in India. Their power to **instantly spread information** has been exploited by various groups, placing them at the center of several national crises.

1. **Misinformation, Disinformation, and Incitement to Violence**

   The most immediate threat from social media is its use to **spread false information** that can provoke real-world violence and communal discord.

Student Notes:

- **Fake News and Propaganda:** A significant portion of **fake news** on Indian social media is political or religious, designed to fuel sectarian divides. This was evident in the **Muzaffarnagar riots (2013)** and the **Dadri lynching (2015)**, where doctored videos and hate speech spread rapidly, playing a key role in mobilizing violence.
- **Deepfakes and AI-driven Threats:** The rise of **Artificial Intelligence (AI)** has introduced **deepfakes**—hyper-realistic but fake videos and audio clips. These can be used to create social polarization, suppress dissent, and manipulate public opinion with frightening authenticity.

Misinformation Deadly Impact: The Dhule Case

The **Dhule Lynchings (2018)** tragically resulted in **5 deaths** in Maharashtra. This brutal incident was directly fueled by **viral WhatsApp rumors** about "child-lifters."

- **Echo Chambers and Polarization:** Social media algorithms often create **filter bubbles** or **echo chambers**, where users are only shown content that reinforces their existing beliefs. This insulates them from different views, **deepens polarization,** and increases the risk of sudden, flashpoint violence.

Recent Threats from Social Media to India's Internal Security

Misinformation During Operation Sindoor (2025): After **Operation Sindoor**, fake claims like "**India seized Karachi**" and "**Pakistani generals arrested**" spread on **X, WhatsApp, YouTube**, and **Facebook**, increasing public **tension** and **risking escalation**.

Deepfake Election Disinformation (2024–2025): **Deepfake videos** featuring celebrities falsely endorsing political parties circulated on **Instagram**, **WhatsApp**, and **Facebook**, triggering police **investigations** and raising concerns about **AI-generated disinformation**, similar to **Cambridge Analytica**.

Communal Rumors & Hate Speech: Platforms like **WhatsApp** and **Facebook** spread fake videos, **provocative messages**, and **hate speech** during events like the **2020 Delhi riots**, **CAA protests**, and **2024 Nuh violence**, escalating tensions.

Public Health Misinformation During COVID-19: **Misinformation** about cures, **anti-vaccine conspiracies**, and false preventive measures spread on **WhatsApp**, **Twitter**, and **YouTube**, undermining **public health efforts** and creating **confusion**.

2. Tool for Radicalization and Extremist Recruitment

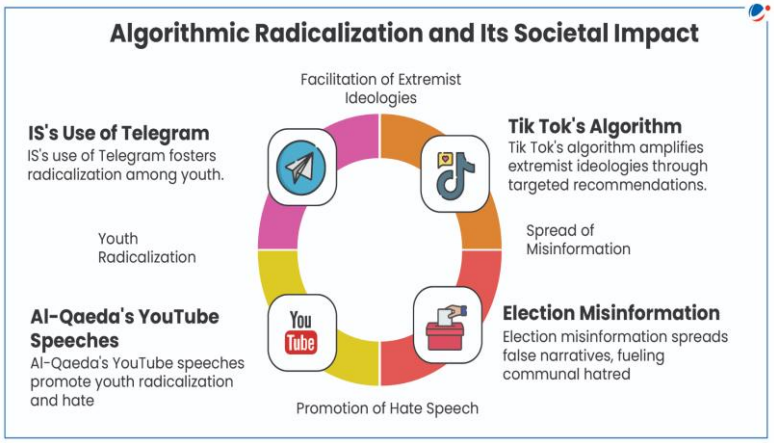
Terrorist and extremist groups have effectively weaponized social media to advance their dangerous agendas.

- **Recruitment and Radicalization:** Groups like **ISIS** have used social media to spread propaganda in Indian languages, including **Hindi** and **Tamil**, to attract and radicalize vulnerable youth.
- **Transnational Threats:** These platforms enable extremists to communicate with **foreign handlers** using encrypted apps, bypassing traditional surveillance and creating a significant transnational threat.
- **Psychological Operations (PsyOps)**: By **live-streaming attacks** and celebrating acts of violence, terrorists aim to **instill fear**, **challenge state legitimacy**, and project an image of **power**, thus attracting more followers.
- **Lone Wolf Attackers:** The "virtual community" on social media is a powerful tool for inspiring individuals to carry out attacks on their own, known as **lone wolf attackers**, who are radicalized entirely online.

The Digital Rabbit Hole: How Algorithms Fuel Radicalization

Social media algorithms are designed to keep us engaged by showing us content we are likely to interact with. However, this same process can lead to **Algorithmic Radicalization**—a dangerous digital "rabbit hole" that pushes users towards **extremist propaganda** and

polarizing views. This creates **echo chambers** and **filter bubbles** that reinforce a user's biases (**confirmation bias**) and can lead them down a path to extremism.



Why It's So Hard to Stop	**Steps are being taken to combat this threat.**
• The algorithms themselves are often complex **"black boxes."** • Extremist groups like **IS** and **al-Qaeda** use coded language and symbols (**modulated content**) to evade automated detection. • There is a constant struggle to balance content **moderation with free speech**. • Algorithms often fail to understand crucial **local contexts** in different countries. • A lack of **international regulation** hinders a unified global response.	• **Globally:** The **EU's Digital Services Act 2023** demands more transparency, platforms like **YouTube** use **AI-driven moderation**, and the **Christchurch Call** forms a global coalition against extremist content. • **In India:** The **Ministry of Electronics and Information Technology (MeitY)** actively flags and removes harmful URLs, and the **IT Rules 2021** provide a legal framework for tracing and removing such content.

3. Foreign Interference and Information Warfare

Hostile state and non-state actors use social media to conduct **information warfare** against India.

- **Influence Operations:** These actors manipulate **hashtags**, promote divisive narratives, and launch coordinated disinformation campaigns to destabilize India's social fabric, particularly during **elections** or major policy debates as seen in 2020–2021 Indian farmers' protest..
- **Anonymity and Impunity:** The borderless nature of social media allows foreign powers to target India's internal discourse with a degree of **anonymity** and impunity, making it difficult to trace the source of the interference.

4. New-Age Cybersecurity and Criminal Threats

Beyond direct violence, social media has opened the door to a new generation of complex security challenges.

- **Cyber Attacks and Financial Fraud:** Social networks are a common pathway for financial crimes. Hackers use these platforms to spread malicious software like the **SOVA Android Trojan**, which targets mobile banking apps, and to carry out **phishing** attacks.
- **Data Colonisation:** Global social media corporations collect massive amounts of data from Indian users. This creates a situation of **"data colonisation,"** where this valuable information is stored and controlled outside the country and could be **manipulated against India's interests.**

Student Notes:

- **Targeting Vulnerable Populations:** Social media is often used to target **women and children** through **cyberbullying**, **doxxing**, and targeted harassment campaigns, causing significant psychological harm.
- **Organized Crime:** The platforms are also used for other illegal activities, including **money laundering** and coordinating criminal operations.

Information Warfare During Operation Sindoor

The military conflict of **Operation Sindoor** was fought just as intensely online. This **"war of perception"** saw both India and Pakistan use social media and digital platforms to control the story and influence global opinion.

Pakistan's Disinformation Strategy	**India's Fact-Based Counter-Narrative**
Pakistan's campaign was a coordinated effort led by its military media wing, the **DGISPR**, to mislead domestic and international audiences. • **Core Narrative:** The main goal was to portray the initial **Pahalgam attack** as a **'false flag'** operation conducted by India and to fabricate stories of military success. • **Digital Tactics:** They used social media platforms like **X (Twitter)** with specific **hashtags**, state-aligned influencers, and automated **botnets** to spread propaganda. • **Visual Deception:** They created **billboards** in Pakistani cities with photoshopped images of downed Indian aircraft and reused old conflict footage, a tactic called **'narrative laundering'**. • **Chinese Support:** This campaign was actively **amplified by Chinese state media**, highlighting a digital nexus between the two countries.	India's official response was led by the military's **ADGPI**, the government's **PIB**, and the **Ministry of External Affairs (MEA)**. • **Core Strategy:** India chose a **'truth-driven approach'**, using facts and evidence to counter lies instead of creating its own propaganda. The message was that India's actions were a **calibrated response** against terror. • **Key Action:** To debunk fake videos of downed helicopters, India released official **timestamped satellite imagery** showing the aircraft returning safely to base. • **Platform Action:** India requested social media platform **X** to block over **8,000 accounts** that were spreading misinformation.

Key Takeaways

- **The Challenge of Speed:** A key criticism noted in the reports was that India's strategic communication, while factual, was sometimes **'clumsy and slow'**, allowing Pakistan's propaganda to spread first. This highlights the need for rapid response in crisis communication.
- **The New Battlefield:** The conflict proved that **information warfare** is a central battlefield. For civil servants, managing this 'war of perception' is as critical as managing the physical conflict itself, as it shapes diplomatic support and domestic morale.

Student Notes:

5.3. Government Measures to Counter Media and Social Media Threats

The Indian government has implemented a multi-pronged and dynamic approach to address the internal security challenges posed by both traditional and new age digital media.

5.3.1. Regulating Traditional and Digital News Media

To ensure responsible reporting and prevent the dissemination of information that could harm national security, the government relies on a set of established laws, regulatory bodies, and direct advisories.

- **Constitutional and Legislative Framework:**
  - **Constitutional Provisions:** While **Article 19** guarantees freedom of speech, it is subject to reasonable restrictions for national security.
  - **Key Statutes:** Laws such as the **Press Council Act of 1978**, **National Security Act of 1980**, **Defence of India Act, 1962**, and the **Civil Defence Act, 1968** provide the legal basis for regulating media content to protect national interests.
- **Regulatory Bodies and Codes:**
  - The **Press Council of India (PCI)** acts as a watchdog for print media ethics. For electronic media, the self-regulatory **Broadcasting Code** and bodies like the **News Broadcasting Standards Authority (NBSA)** and the **Indian Broadcasting Foundation (IBF)** set content guidelines.
- **Direct Media Advisories:** During national security operations, the government issues specific **advisories to news channels** to exercise discretion and avoid live coverage that could reveal sensitive operational details or amplify unverified information.
- **Judicial Intervention:** The **Supreme Court** has repeatedly guided media conduct, notably criticizing the live coverage of the **26/11 Mumbai terror attacks** for jeopardizing national security.

5.3.2. Tackling Threats from Social Media and Online Platforms

Recognizing the unique challenges of speed and anonymity on social media, the government has adopted a strategy combining legal tools, active monitoring, public awareness, and technological adaptation.

- **Legal Tools for Online Regulation:**
  - **The Information Technology (IT) Act, 2000: Section 69A** is actively used to block fake content and malicious websites.
  - **IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021:** These rules are critical for regulating social media platforms, mandating the swift removal of misinformation and the appointment of **grievance redressal officers**. These tools have been deployed during events like **Operation Sindoor** to manage the information space.
- **Active Counter-Measures and Fact-Checking:**
  - **Fact-Checking and Debunking Propaganda:** The **Press Information Bureau (PIB) Fact Check Unit** serves as a vital instrument in combating misinformation. For instance, it played a key role in debunking several **Pakistani propaganda claims** following security operations, including false reports about downed **Rafale jets** or Indian military surrender.
  - **Monitoring and Blocking Harmful Accounts:** Authorities actively identify and block thousands of influential **Pakistan-linked social media handles** and accounts found spreading misinformation and communal hatred, especially during major crises like the **CAA protests** and other violent incidents.
  - **Banning Anti-National Content:** The government has blocked numerous **YouTube channels** and other online resources found to be spreading anti-India propaganda.

Student Notes:

- **Technological Infrastructure and Surveillance:**
  - India has bolstered its e-surveillance capabilities with projects like the **National Intelligence Grid (NATGRID)**, **Central Monitoring System (CMS)**, and **Network Traffic Analysis (NETRA)**.
  - Specialized agencies like **CERT-In** (Indian Computer Emergency Response Team) and the **National Critical Information Infrastructure Protection Centre (NCIIPC)** form the core of the nation's cybersecurity defense.
- **Public Awareness and Citizen Vigilance:**
  - The government has initiated official campaigns urging citizens to verify information before sharing and to report dubious content. Public calls to use official portals like **PIBFactCheck** and dedicated reporting channels on **WhatsApp** and email foster a grassroots approach to tackling fake news.
- **Addressing Emerging Challenges:**
  - The government remains focused on updating regulations to counter new and evolving threats. This includes policy considerations for tackling **AI deepfakes** and continuously strengthening national cybersecurity measures to stay ahead of sophisticated threats.

Way Forward: Key Recommendations to Strengthen Internal Security

To tackle evolving threats from **media** and **social networking sites**, a **multi-dimensional strategy** is essential, focusing on strengthening **legal frameworks**, enhancing **technological capabilities**, and promoting **public awareness**.

Strengthening Institutional and Legal Frameworks:

- **Empower Regulatory Bodies**: Grant **Press Council of India** (PCI) statutory powers and consider granting statutory status to the **News Broadcasters Association** (NBA).
- **Independent Industry Regulator**: Establish a body to enforce **media ethics** with powers to impose fines for violations.
- **National Social Media Policy**: Create a comprehensive **Social Media Policy** to tackle platform-specific challenges.
- **Code on Disinformation**: Adopt a formal **code on disinformation** similar to the EU's, disrupting revenue for fake news.
- **Regulate Media Trials**: Establish clear rules to balance **free speech** with the **right to a fair trial**.
- **Strengthen Data Protection Laws**: Enhance **personal data protection** and define **data ownership** clearly.

Enhancing Technological and Intelligence Capabilities:

- **Boost Domestic Data Infrastructure**: Support **local data centers** with energy and connectivity.
- **Develop Advanced Intelligence Models**: Utilize **SOCMINT** for predictive tools to monitor and prevent risks.
- **Expand Pilot Projects**: Launch **social media pilot projects** for better data and intelligence.

Fostering Public-Private Collaboration and Awareness:

- **Empower Agencies and Build Talent**: Equip government agencies with **legal** and **technical** expertise.
- **Increase Public Awareness**: Educate citizens on the risks of **social networking** and **privacy**.
- **Promote Corporate Responsibility**: Encourage corporations to adopt revised **security models** for information sharing.

Student Notes:

UNIT 4: MONEY LAUNDERING AND ITS PREVENTION, AND LINKAGES OF ORGANIZED CRIME WITH TERRORISM

"Money laundering is the financial reflex to crime" -FATF Report

Previous Years Question

- **(2023)** Give out the major sources of **terror funding** in India and the efforts being made to curtail these sources. In the light of this, also discuss the aim and objective of the No Money for Terror (NMFT) Conference recently held in New Delhi in November 2022. (250 words/15m)
- **(2021)** Discuss how emerging technologies and globalisation contribute to **money laundering**. Elaborate measures to tackle the problem of money laundering both at national and international levels. (150 words)
- **(2018)** India's proximity to two of the world's biggest illicit **opium-growing states** has enhanced her internal security concerns. Explain the linkages between **drug trafficking** and other illicit activities such as gunrunning, money laundering and human trafficking. What counter-measures should be taken to prevent the same?
- **(2013) Money laundering** poses a serious threat to a country's economic sovereignty. What is its significance for India and what steps are required to be taken to control this menace?

1. Money Laundering

Money laundering is a **clandestine** and **complex process** that forms the bedrock of almost all **profit-generating criminal activities**. It is not merely an **economic offense** but a **grave threat** to a nation's **financial sovereignty** and **internal security**.

Essentially, **money laundering** is the process of making **"dirty money" (money from crime) look "clean"** (like it's from a legal source). It involves three main actions:

Panama Papers (2016): Offshore Secrets Exposed

The **Panama Papers (2016)**, a massive leak, exposed how **global elites** used **shell companies** via Mossack Fonseca to potentially hide **$2.1 trillion in assets**, often for **tax evasion** and **money laundering**.

In response, **India** launched **150+ investigations** into individuals linked to the leaks, demonstrating a significant effort to tackle **illicit financial flows** and undisclosed offshore wealth.

1. **Conversion:** Actively moving or changing money to hide its criminal source, or helping the criminals involved avoid getting caught.
2. **Concealment:** Intentionally hiding the truth about dirty money, such as who really owns it or where it came from.
3. **Acquisition:** Simply accepting, holding, or using any money or property that you know is the result of a crime.

India's primary legislation, the **Prevention of Money Laundering Act (PMLA), 2002**, defines the offense of money laundering in a comprehensive manner. It states:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any

***process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of the offense of money-laundering."*-PMLA Section 3**

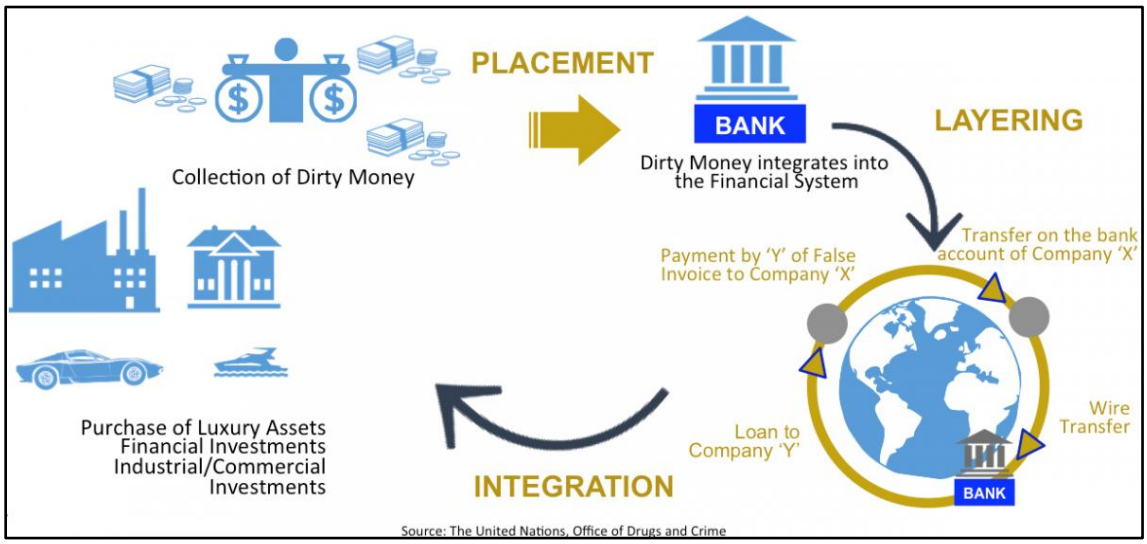
The scale of **money laundering** is staggering, posing a significant threat to the global economy.

- **Global Estimates**: The **International Monetary Fund (IMF)** estimates that the aggregate amount of money laundered globally in one year is between **2 to 5 percent** of the world's **Gross Domestic Product (GDP)**.
- **Indian Context**: The **UN Office on Drugs and Crime (UNODC)** has estimated that criminal proceeds in India could account for as much as **4.6%** of the country's **GDP**.
    - The **Basel Anti-Money Laundering (AML) Index** has also consistently ranked India among countries with a significant risk of money laundering.

1.1. The Three-Stage Process of Money Laundering

"Placement, Layering, Integration: The 'lifecycle' of dirty money"

Money laundering is typically carried out in three distinct stages- **Placement, Layering and Integration**, each designed to progressively obscure the illicit source of the funds.



1. **Placement:** First, criminals **place** the **dirty money** into the financial system. They often break up large amounts into smaller, less suspicious deposits to avoid detection.
2. **Layering:** Next, they create a complex web of transactions to hide the money's origin. This **layering** involves multiple bank transfers and buying assets to make the trail impossible to follow.
3. **Integration:** Finally, the now "clean" money is **integrated** back into the legitimate economy. It appears legal and can be spent or invested freely.

1.2. The Evolving Modus Operandi of Money Laundering

Without dirty money, crime wouldn't pay" – Stolen Asset Recovery Initiative (World Bank/UNODC)

Student Notes:

Student Notes:

1.2.1. Traditional Approaches of Money Laundering

1. **Structuring/Smurfing**

   This technique involves **breaking down large amounts of cash into smaller deposits** below the mandatory reporting threshold of financial institutions. Multiple individuals, known as **"smurfs"**, make these deposits into various bank accounts to avoid detection.

Sahara's Money Laundering Allegations

The **Sahara Group Case (2013)** illustrates alleged money laundering. Illicit funds were routed through **34,000 shell companies (Placement)**, introducing them into the system and obscuring their origin.

Subsequently, these funds were sent via **offshore entities (Layering)** to hide their trail. Finally, the money was integrated back into the legitimate economy by purchasing **luxury hotels (Integration)**, providing a clean façade for illicit wealth.

2. **Hawala**

   "No records, no trail, just trust; Moving millions in the shadows' dust."

   Hawala is an informal, **parallel remittance system** that operates outside the formal banking network. It involves a network of **hawaladars** who transfer value across borders without physical currency, making it untraceable. It is banned in India under **PMLA** and **FEMA**.

India's Hawala Scandal: A Web of Politics and Terror

The **1991 Hawala Scandal** was a major corruption case in **India** where top **politicians** and **bureaucrats** secretly received illegal payments.

The money was funneled through **hawala brokers**, primarily the **Jain brothers**.

The scandal came to light after the arrest of **Ashfak Hussain Lone**, a member **Hizbul Mujahideen**. He revealed that his organization was also receiving funds through these same **hawala channels**.

This directly linked political **corruption** with **terrorist financing**.

The 26/11 Attacks: Funded Through Hawala

The tragic **26/11 Mumbai Attacks** of 2008 were paid for using the **Hawala** system, with funds coming from **Pakistan**.

This shadow banking network allowed the terror group **Lashkar-e-Taiba** to secretly send **untraceable money** for their **cross-border terror operations**. The attack was a powerful example of how **Hawala** serves as a dangerous financial tool for **illicit activities**.

3. **Trade-Based Money Laundering (TBML)**

   TBML disguises illicit proceeds through legitimate trade transactions, including:

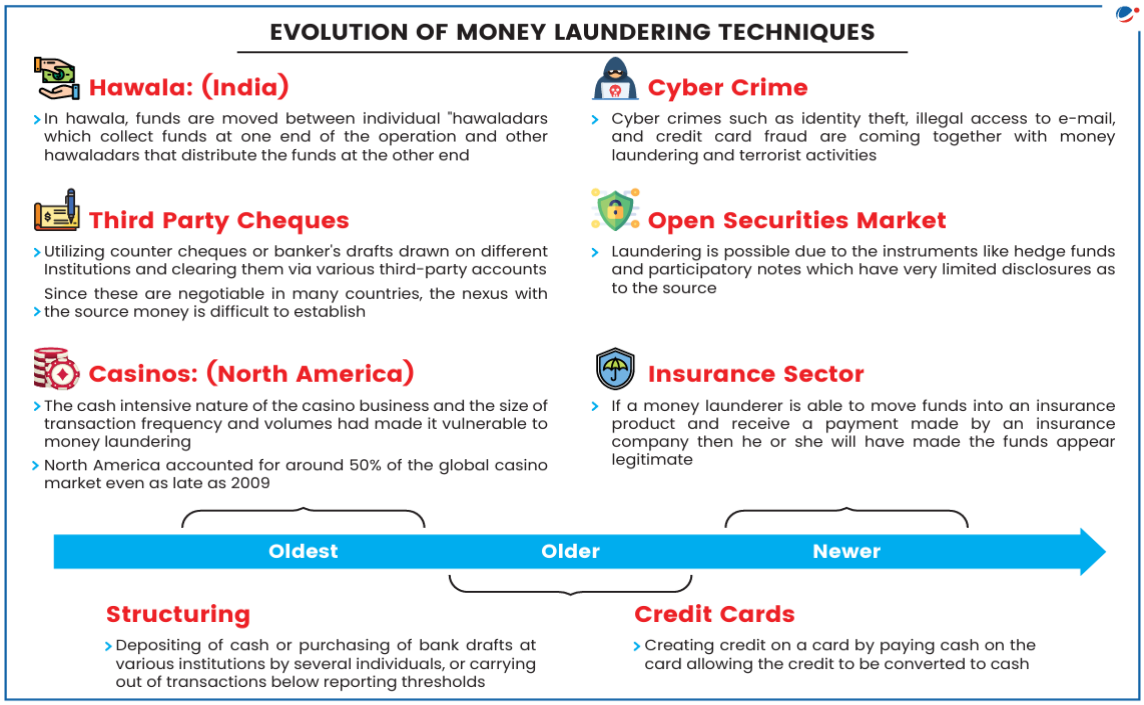
   - **Over-invoicing or under-invoicing** of goods and services.
   - **Issuing multiple invoices** for the same shipment.
   - **Falsifying goods or services descriptions**.

4. **Use of Shell Companies and Third-Party Cheques**

   Shell companies are fictitious entities used to create fake invoices and transactions, making illicit funds appear legitimate. Third-party cheques are also used to disguise the real origin of funds.

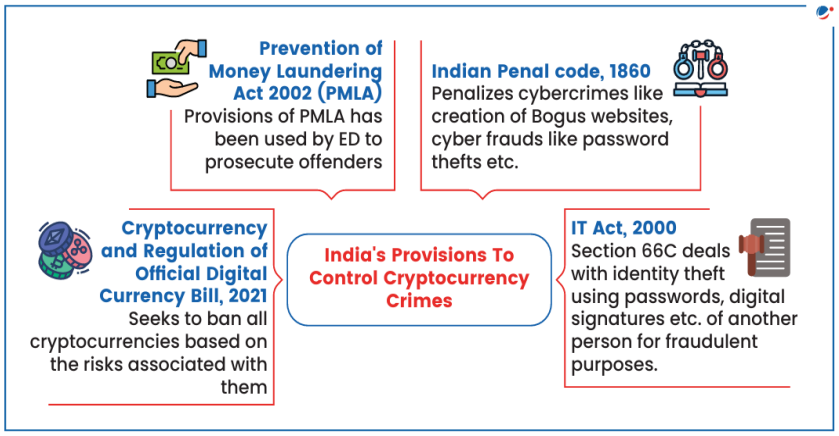
5. **Use of Cash-Intensive Businesses**

   Businesses dealing with large volumes of cash, such as **casinos**, **restaurants**, and **real estate**, are used to mix illicit funds with legitimate revenue, making the dirty money harder to trace.



1.2.2. Modern Approaches of Money Laundering

1. **Cryptocurrencies**



Cryptocurrencies, like **Bitcoin**, offer a new tool for money launderers due to their **pseudo-anonymous** nature.

- Launderers use **mixers** or **tumblers** to pool and redistribute cryptocurrency, breaking the link between the original source and final destination.
- In 2021, illicit transactions using cryptocurrencies were estimated at **$14 billion** globally.

In the **WazirX case** (2021), India's **The Enforcement Directorate (ED)** froze over **₹64 crore**, showing how easily **cryptocurrency** can be used for **money laundering**. While publicly linked to **loan app frauds**, the case highlighted the broader problem of hiding **illicit proceeds** in **digital assets**.

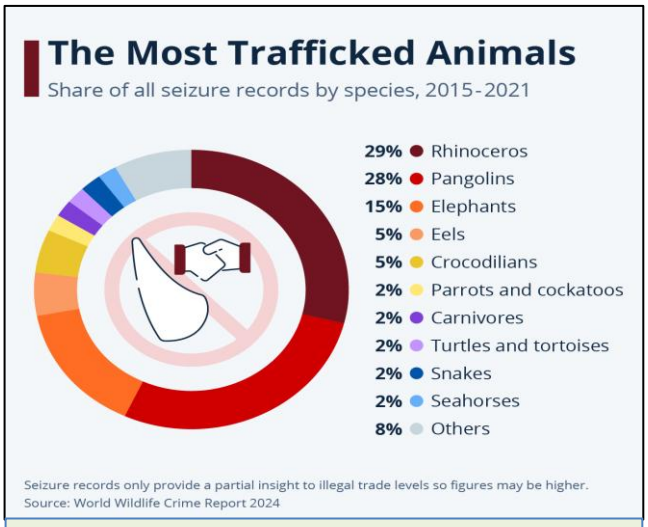
2. **Cybercrime**

Cybercrime proceeds, such as funds from **hacking**, **phishing scams**, or **ransomware attacks**, are laundered via complex digital pathways, often involving **multiple jurisdictions** to **obscure the origin of the funds.**

3. **Linkages with Illegal Wildlife Trade (IWT)**

The **Illegal Wildlife Trade (IWT)** is more than just an environmental issue; it's a massive criminal enterprise that generates billions in **illicit proceeds**.

- To "clean" this dirty money, traffickers use classic **money laundering** tactics. They hide the cash using **front companies**, like private zoos or farms, and wire the funds through countries with **weak enforcement**.
- In **India**, wildlife traffickers are deeply **connected** to powerful **organized crime networks**. These are often the same groups involved in **human trafficking**, **illicit drugs**, and **corruption**.
- **Illegal wildlife trade** in India is a high-profit, low-risk activity linked to **terrorism** and **insurgency**.
    - **Wildlife trafficking syndicates** fund militant groups, especially in **Northeast India**. Poaching profits are used for **arms purchases** and **terror activities**.
    - **Trafficking routes** overlap with those used for **drugs**, **arms**, and **human trafficking**.



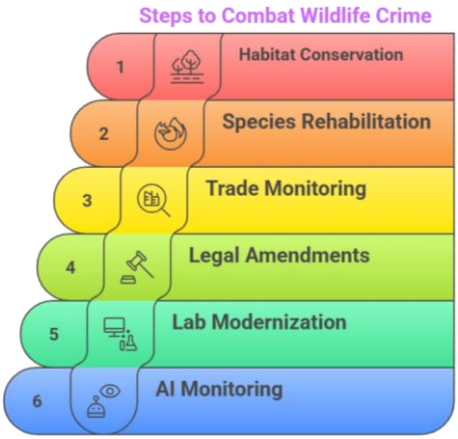
The **World Wildlife Crime Report 2024** shows which animal products are most illegally traded around the globe, revealing this is a major business that fuels **organized crime**.

The report underscores the devastating **twin impacts of this trade**: it pushes **endangered species** toward extinction while funding **dangerous criminal networks** worldwide.

4. **Misuse of the Insurance Sector and Open Securities Market**

   Launderers misuse the **insurance sector** by buying policies with illicit funds and making fraudulent claims.

   - In the **securities market**, they engage in complex transactions involving **hedge funds**, **derivatives**, and **Participatory Notes (P-Notes)** to launder money.



1.3. The Multifaceted Impact of Money Laundering

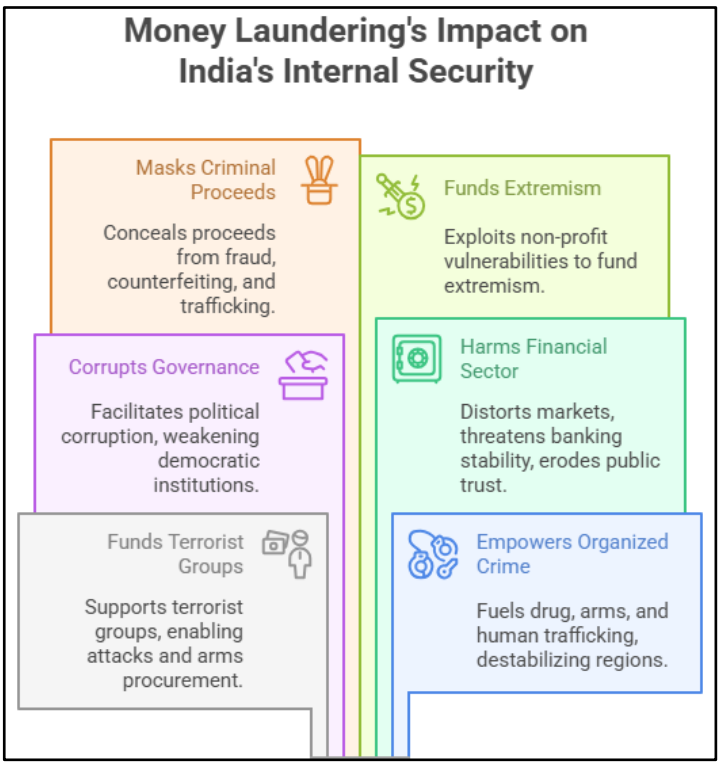
"Ill-gotten gold paves highways to hell" – Adaptation from Tirukkural (Verse 281)

Money laundering is more than just a financial crime; it deeply harms a nation's economy, political system, and social values, posing a major threat to **internal security**.

Economic Impact

- **Hurts Legitimate Businesses:** Criminals use laundered money to fund their front companies, allowing them to sell goods below market price and drive honest, **legitimate businesses** into the ground.
- **Disrupts Financial Markets:** Large flows of dirty money can cause chaos in **financial markets**, leading to unstable **exchange rates** and **interest rates**.
- **Reduces State Revenue:** Since this money is hidden, it isn't taxed, leading to a massive loss of **state revenue** that could have funded public services.

- **Damages Reputation:** A reputation for corruption scares away crucial **Foreign Direct Investment (FDI)** and harms the credibility of the nation's financial institutions.



Political Impact

- **Fuels Corruption:** Dirty money is used to bribe **public officials**, police, and judges, weakening the state from the inside.
- **Criminalizes Politics:** It leads to illegal **electoral funding**, creating a system where criminals can buy political power. A key example is the **Narada Sting (2016)**, which caught **TMC ministers** in **West Bengal** on camera accepting bribes, directly linking laundered money to the **criminalization of politics**.

Social Impact

- **Damages the Social Fabric:** It sends the message that crime pays better than honest work, eroding ethical standards.
- **Empowers Criminality:** By making crime so profitable, it encourages a rise in **drug addiction**, **violence**, and a general breakdown of law and order.

Student Notes:

1.4. Key Challenges in Prevention of Money Laundering

India's fight against money laundering continues to face significant hurdles despite its strong legal and institutional frameworks. A few critical challenges include:

- **The Rapid Pace of Technological Change:** Emerging technologies like **cryptocurrencies**, the **darknet**, and **AI-driven tools** are providing sophisticated and anonymous avenues for laundering money. These technologies outpace the current capabilities of enforcement agencies.
- **The Challenge of Tax Havens and Financial Secrecy:** Countries with **tax havens** and **offshore financial centers** often have stringent secrecy laws, making it hard to trace illicit funds or identify the **ultimate beneficial owners**.
- **Lack of Awareness and Weak Compliance Culture:** There is a **lack of awareness** about **AML (Anti Money Laundering)/CFT obligations** in certain sectors, particularly among **non-financial businesses** and professionals. This ignorance, combined with a **weak compliance culture**, leaves gaps that criminals can exploit to launder money without detection.
- **Issues with Inter-agency Coordination and Resource Constraints:** Tackling money laundering requires **seamless inter-agency coordination**. However, coordination issues persist between central and state agencies, hindering real-time information sharing. Additionally, agencies face **resource and manpower constraints** to combat money laundering operations.

1.5. The Global Fightback: International Mechanisms for Prevention of Money Laundering

Since **money laundering** is a borderless crime that exploits the global financial system, **international cooperation** is crucial for combating it effectively. Several key international mechanisms and conventions form the foundation of this global fight

1.5.1. The Financial Action Task Force (FATF)

"Follow the money, find the terror" – FATF guiding principle (1989).

The FATF, established in **1989**, is the most prominent inter-governmental body combating **money laundering (AML- Anti Money Laundering)** and **terrorist financing (CFT- Countering the Financing of Terrorism)**. Its primary role is to promote effective implementation of legal, regulatory, and operational measures.

FATF Flags Digital Terror Funding

The **FATF** warns that **e-commerce platforms** and **online payment services** are being abused for **terror financing**, citing the **Pulwama (2019)** and **Gorakhnath (2022)** attacks. The watchdog also flags **state sponsorship of terrorism**.

Following the **Pahalgam attack (April 2025)**, India requested **Pakistan's** re-listing on the **FATF Grey List**, highlighting ongoing cross-border terror funding concerns.

- **FATF Recommendations**: The FATF has issued **40 Recommendations**, the international standard for AML/CFT, covering everything from criminalizing money laundering to establishing a **Financial Intelligence Unit**.
- **Black and Grey Lists**: The FATF monitors countries' compliance and publicly identifies jurisdictions with deficiencies.
    - **Grey List**: Countries placed under increased monitoring, required to resolve deficiencies with an action plan.
    - **Black List**: Countries, like **North Korea** and **Iran**, face severe global financial countermeasures.

Student Notes:

1.5.2. Key International Conventions

International Conventions provide a global framework for combating **money laundering**, **corruption**, and **organized crime**. These treaties set legal standards for member states to address illicit financial flows

- **UN Vienna Convention (1988):** The **UN Vienna Convention** was the first international agreement to tackle **money laundering** linked to **drug trafficking**, requiring member states to criminalize such activities.
  - Criminalizes laundering of proceeds from **drug trafficking**.
  - Paved the way for **global cooperation** on narcotic-related financial crimes, fostering international cooperation through mechanisms like **extradition**, **mutual legal assistance**, and **confiscation** of proceeds of crime.
  - Provides foundation for future treaties and frameworks on **anti-money laundering**.
- **UN Palermo Convention (2000):** The UN Palermo Convention **expanded the scope of money laundering to include proceeds from all serious crimes**, providing a comprehensive framework for combating organized crime.
  - **Criminalizes laundering** of proceeds from all **serious crimes**, not just drugs.
  - Emphasizes **international collaboration** and harmonization of laws.
  - Key tool in addressing **transnational crime** and **money laundering**.
- **UN Convention Against Corruption (2003):** The UN Convention Against Corruption focuses on curbing corruption globally, promoting cooperation and the recovery of illicit assets.
  - Addresses **corruption** and promotes **asset recovery**.
  - Encourages **international collaboration** in corruption-related prosecutions.
  - Supports **transparency** and **accountability** in public institutions

Global Oligarch Asset Freeze

Following **Russia's 2022 Ukraine invasion**, **Western nations** launched unprecedented **global efforts** to **freeze Russian oligarch** and state-owned **assets**. This **ongoing initiative** aims to cripple Russia's economy, leveraging **international cooperation** among agencies like **Financial Intelligence Units (FIUs)** and **Interpol**.

These global efforts emphasize **intelligence sharing**, **dark web monitoring**, and **international collaboration** to trace **illicit financial flows**.

India can learn to strengthen its **financial intelligence** for combating **cross-border illicit finance** and **organized crime**.

1.5.3. Other Global Initiatives

- **The Egmont Group**: A network of **165 Financial Intelligence Units (FIUs)** facilitating secure information exchange to trace illicit financial flows. India's FIU-IND is an active member.
- **Asia-Pacific Group on Money Laundering (APG)**: As a **FATF-Style Regional Body (FSRB)**, India works with regional partners to implement FATF standards.
- **Basel Committee's Principles**: Provides guidelines for banks on preventing the criminal use of their facilities, focusing on **Customer Due Diligence** and cooperation with law enforcement.

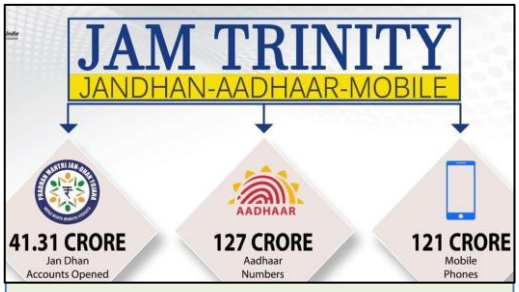
1.6. India's Legal and Institutional Framework Against Money Laundering

***"Laundering isn't finance—it's violence turned to numbers."* – core message of Global Financial Integrity Report 2025**

India has developed a robust legal and institutional framework to combat the growing threat of money laundering, ensuring compliance with international standards while safeguarding its financial integrity. This framework focuses on **detection, investigation,** and **prosecution** of financial crimes.

Student Notes:

1.6.1. Primary Legal Instrument: PMLA, 2002



JAM Trinity's Impact

India's **JAM Trinity (Jan Dhan-Aadhaar-Mobile)** significantly impact on **cash laundering** (e.g., a "15% reduction" by RBI 2024)

Crucially, JAM enabled **direct tracking of 440 million subsidies**, leading to authentic and substantial savings of **₹1.78 lakh crore** for the government by eliminating leakages and corruption.

Key Provisions

The Prevention of Money Laundering Act (PMLA), 2002, is the cornerstone of India's anti-money laundering efforts.

- **Criminalizes Money Laundering**: The Act criminalizes money laundering as a cognizable and non-bailable offense.
- **Obligations on Reporting Entities**: Banks, financial institutions, and intermediaries are required to perform KYC checks, maintain transaction records, and report suspicious activities to the Financial Intelligence Unit (FIU-IND).
- **Powers of Attachment and Confiscation**: The Enforcement Directorate (ED) has the authority to attach and confiscate property derived from proceeds of crime.
- **Special Courts**: Special Courts are established to expedite trials for PMLA offenses.

Recent Amendments

- **Expanded Definition of "Proceeds of Crime"**: Now includes property related to scheduled offenses.
- **Money Laundering as a Stand-Alone Crime**: A conviction for the predicate offense is no longer required for pursuing money laundering charges.
- **Lowered Threshold for Beneficial Ownership**: The definition of "beneficial owner" is tightened from 25% to 10% ownership.
- **Inclusion of New Entities**: The reporting entities now include professionals (e.g., chartered accountants) and transactions involving virtual digital assets (VDAs).

PMLA: Expanding its Digital Reach

India's PMLA (2002) is the nation's key **anti-money laundering** law. Crucially, the Ministry of Finance's **March 2023 notification** explicitly brought **Virtual Digital Assets (VDAs)**, including **cryptocurrencies** and **NFTs (Non Fungible Tokens)**, under its purview.

This allows the **ED** to **seize** such **virtual assets**, bolstering India's efforts to combat **money laundering** in the digital realm, aligning with global standards.

1.6.2. Institutional Mechanisms against Money Laundering

- **Financial Intelligence Unit - India (FIU-IND):** Established in 2004, FIU-IND is the central agency for India's anti-money laundering efforts. **Functions**:
  - Collects financial data like **Cash Transaction Reports (CTRs)** and **Suspicious Transaction Reports (STRs)**.
  - Analyzes data to identify illicit financial activities.
  - Shares actionable intelligence with law enforcement agencies.
- **Enforcement Directorate (ED):** The ED investigates money laundering offenses under the PMLA and prosecutes offenders in special courts. It is India's primary agency for handling financial crimes.
  - **ED's Broadened Powers:** The **Vijay Madanlal Choudhary vs. The UoI (2022)** case was a **landmark Supreme Court judgment** that **upheld** the **Enforcement Directorate's (ED)** significant **arrest powers** under **Section 19** of the **PMLA, 2002**. This ruling significantly **strengthened** the **ED's** hand in combating **money laundering**, validating its broad authority in investigations, arrests, and asset seizures under the Act.

Student Notes:

1.6.3. Supporting Legal Frameworks

In addition to the PMLA, other legal instruments play a vital role in combating money laundering:

Foreign Exchange Management Act (FEMA)

The **Foreign Exchange Management Act (FEMA)**, introduced in **1999**, is India's primary law for managing all foreign currency transactions. Its main purpose is to facilitate international trade and investment while maintaining a stable foreign exchange market, all under the regulation of the **Reserve Bank of India (RBI)**.

How FEMA Helps Prevent Money Laundering:

FEMA helps prevent **money laundering** by creating a legal and documented framework for all money moving across India's borders.

- **Creates a Paper Trail:** By forcing foreign exchange transactions into official, regulated channels, FEMA ensures there is a clear record. This makes it very difficult for criminals to secretly move illicit funds.
- **Flags Illegal Activity:** Any transaction that doesn't follow FEMA's strict rules is immediately flagged as illegal, helping authorities detect suspicious financial activity.

Violating FEMA rules results in heavy penalties and fines, acting as a strong deterrent against the illegal movement of money.

Black Money (Undisclosed Foreign Income and Assets) Act, 2015

Black Money Act (2015) is a powerful law designed to target citizens who illegally hide **undisclosed foreign income and assets**.

It directly prevents **money laundering** by attacking a key part of the process: stashing illicit funds abroad. The Act does this in two main ways:

1. **Creates Severe Deterrence:** It imposes crippling financial consequences on offenders—a flat **30% tax** and an additional penalty of up to **90%** on the hidden asset, plus the threat of **imprisonment** for up to 7 years. This makes the risk of holding black money overseas extremely high.
2. **Forces Financial Transparency:** The law requires Indian residents to declare all their foreign holdings. This destroys the secrecy that criminals need to successfully hide and "clean" their illegal wealth.

The **Benami Transactions (Prohibition) Act, 1988**

The act targets property held in a fake name or in the name of a proxy (**Benamidar**) to hide the identity of the real owner. This Act is a powerful tool against **money laundering** because it directly attacks a common method criminals use to hide their ill-gotten wealth.

It prevents money laundering by:

1. **Breaking the Ownership Chain:** Launderers often buy assets in someone else's name to disconnect themselves from the dirty money. The Act makes this core act of hiding behind a proxy illegal, destroying the anonymity criminals rely on.
2. **Creating Severe Deterrence:** The law's biggest threat is **confiscation**—the government can simply take away the entire benami property. On top of losing the asset, the real owner faces **imprisonment** for up to 7 years and a heavy **fine** of up to 25% of the property's market value.

This risk of total asset loss makes using benami transactions an extremely dangerous and unattractive way to launder money.

Student Notes:

Public Gambling Act, 1867

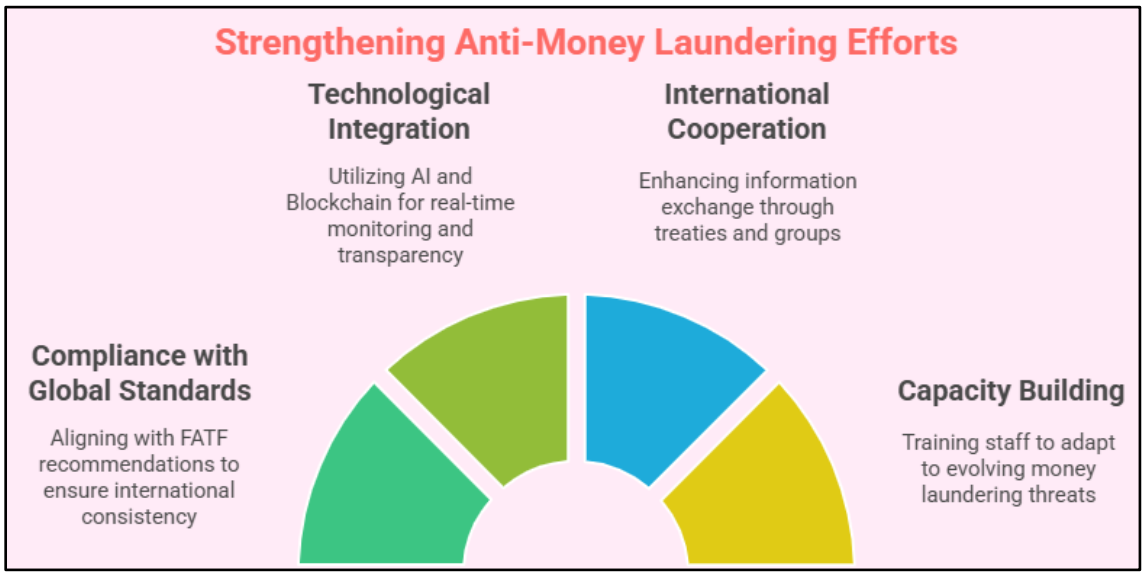
It helps tackle **money laundering** by acting as the legal "key" that unlocks the more powerful **Prevention of Money Laundering Act (PMLA)**.

1. Authorities can use the old **Gambling Act** to establish that an operation is an illegal crime.
2. This initial crime then gives them the legal grounds to launch a full-scale **PMLA** investigation to trace and seize the laundered money from that illegal activity.

A perfect example is the **2023 Probo Media Technologies case**. The **Enforcement Directorate (ED)** first identified the platform's "opinion trading" as a form of illegal gambling. This allowed them to then apply the **PMLA** and freeze **₹284.5 crore** in assets linked to the alleged **money laundering** scheme.

1.7. Strengthening Anti-Money Laundering Efforts

To effectively combat money laundering, India needs to take a **multifaceted approach**, addressing both domestic challenges and global best practices.



2. Linkages of Organized Crime with Terrorism

Organized crime refers to **serious criminal activities** committed by a **group of three or more persons**, structured and coordinated to obtain **financial or material benefits**, as per the **UN Convention against Transnational Organized Crime**. These groups have a clear existence over time and operate with **intentional planning**.

Organized Crime Groups (OCGs) are essentially criminal enterprises built to last. Here's what defines them:

The Rise of Cybercrime-as-a-Service

Cybercrime-as-a-Service (CaaS) is a dangerous trend where hacking tools and services are rented out on **dark web** marketplaces.

This model allows **Organized Crime Groups (OCGs)** and criminals with little technical skill to easily launch sophisticated attacks, dramatically **lowering the barrier to entry** for cybercrime. These criminal platforms offer ready-to-use products like:

- **Ransomware Kits** to lock data for payment,
- **Phishing Kits** to steal credentials with fake websites,
- Access to **Hired Hackers** for specific jobs, and
- **Botnets for Rent** to launch website-crashing **DDoS attacks**.

Student Notes:

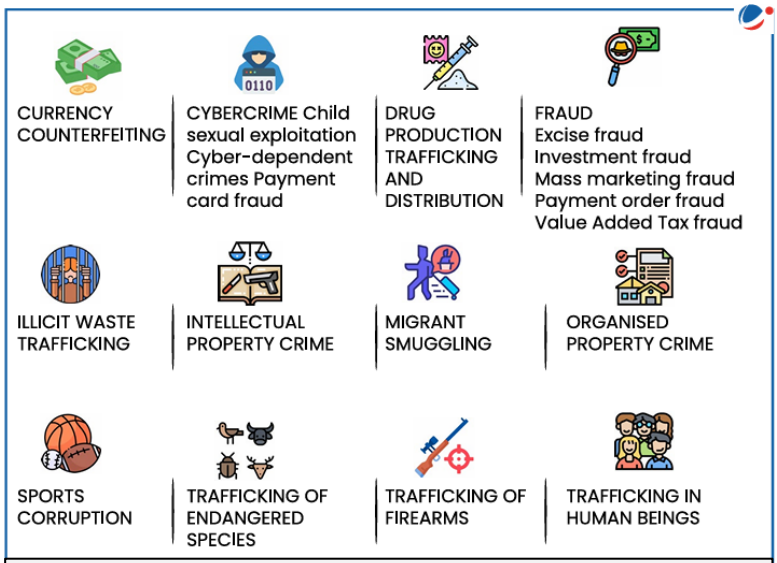
- **Structure and Goal:** They are structured like a real business, with clear ranks and roles.
  - Designed for **continuity** so they can outlive any single member.
  - Their fundamental motive is simple: **profit** from illegal activities.
- **How They Operate:**
  - **Strict Membership:** They are selective about who can join, often based on shared ethnicity or a criminal background.
  - **Modern Technology:** They use advanced tools like social media and the **dark web** to communicate and operate in **secrecy**.
  - **Violence and Bribery:** They use **violence** and threats to enforce discipline and protect their interests. They also **infiltrate** and **bribe** officials to look the other way.
  - **Meticulous Planning:** Their criminal activities aren't random; they are carried out with careful and detailed planning.

'Ndrangheta: Europe's Cocaine Kingpin

The **'Ndrangheta** is a powerful **Italian mafia** group that acts as Europe's cocaine kingpin, controlling an estimated **80% of the continent's cocaine trade**.

Operating globally in over **40 countries**, its annual revenue reaches a staggering **€60 billion**.

Their immense power comes from a unique combination of a secretive, **clan-based structure** and deep **political infiltration** and corruption.



Various Types Organised Crimes

In the Indian context, organized crime is not only about **financial gains**. Activities such as **rigging elections**, **manipulating public opinion**, or fostering **caste-based violence** have also been categorized as **organized crime** when they are carried out systematically by criminal gangs.

2.1. Major Forms of Organized Crime in India

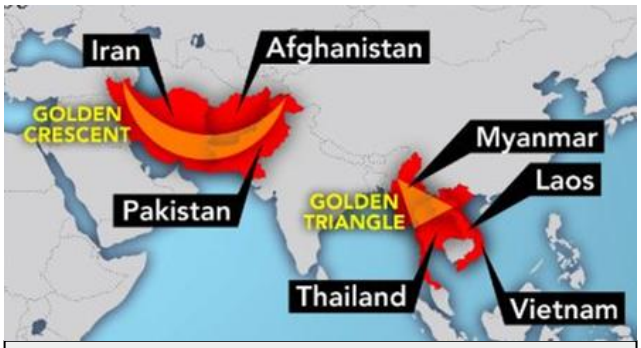
Drug trafficking sustains terror like oxygen sustains fire" – India's UNSC Statement (2020) on narco-terrorism in Punjab and J&K

The following major forms of organized crime are particularly relevant in India, with some closely tied to **terrorism**:

- **Drug Trafficking**: India's strategic position between the **Golden Triangle** (Myanmar, Thailand, Laos) and the **Golden Crescent** (Iran, Afghanistan, Pakistan) makes it a significant **transit point** for narcotics, including **heroin**, **hashish**, **opium**, and **methamphetamine**. The illicit drug trade leads to several **security threats**, including **narco-terrorism**, **social crimes**, and **corruption**.
- **Arms Smuggling**: The illegal trade of **weapons**, explosives, and advanced technology is prevalent across India's porous borders, particularly with **Pakistan**, **Bangladesh**, and **Myanmar**.

Student Notes:

- **Human Trafficking**: This involves the recruitment, transport, and exploitation of people through **coercion**, **fraud**, or **abduction**. India serves as a **source**, **destination**, and **transit** point for **human trafficking**, with various states, including **Assam**, **West Bengal**, **Tamil Nadu**, and **Telangana**, reporting high numbers of cases.

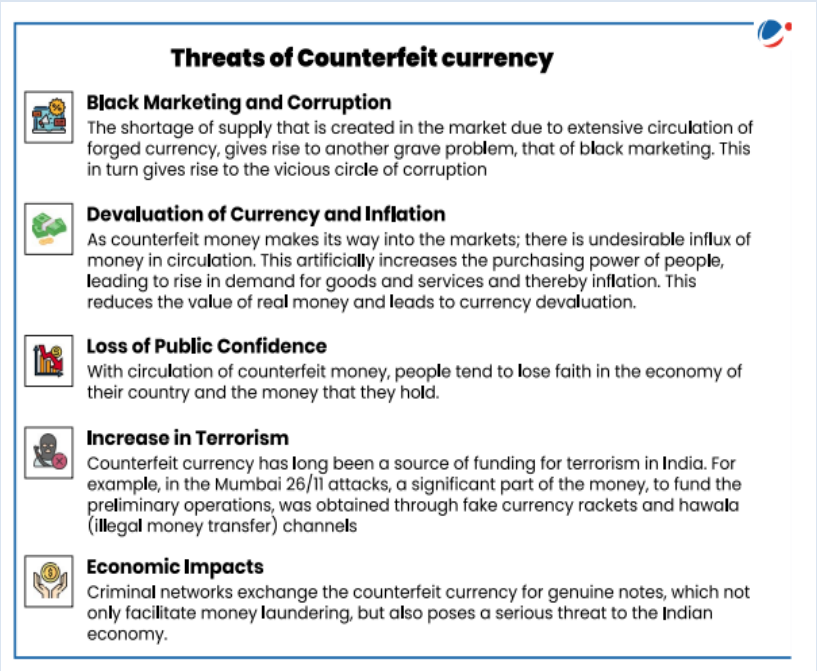


Golden Triangle and Golden Crescent

- **Counterfeiting (Fake Indian Currency Notes - FICN)**: The **counterfeiting** of currency, particularly **FICN**, is a significant source of **terrorist financing**, especially in **Kashmir**. FICN is often **smuggled** into India via **Nepal**, **Bangladesh**, and **Pakistan**. The Ministry of Home Affairs (MHA) has set up the **FICN Coordination Group (FCORD)** to tackle the issue through **intelligence sharing**.
- **Cybercrime**: Cyber-related threats, such as **hacking**, **social engineering**, **cyber-attacks**, and **financial frauds**, have become increasingly prominent in the digital era. These crimes not only undermine **economic stability** but also pose serious **national security threats**.
- **Extortion and Kidnapping for Ransom**: Particularly in regions like **Northeast India**, extortion is used to fund **terrorist activities**. **Kidnapping** for **ransom** is also employed to generate funds for **terrorist groups**.

The Challenge of Counterfeit Currency in India

Counterfeit currency, or **Fake Indian Currency Notes (FICN)**, is the illegal imitation of real money, created with the intent to deceive. This is a serious threat that undermines the economy and is often linked to organized crime and terrorism.



The Scale of the Problem and Demonetisation

By **2016**, India was facing a severe counterfeit currency crisis. At its peak, an estimated **250 out of every 10 lakh** notes in circulation were fake. To combat this widespread problem, the government took the drastic step of **demonetisation** in November 2016, scrapping the old **₹500** and **₹1,000** banknotes.

The value of FICN *seized by law enforcement* has surged, rising from **₹28 crore** in 2017 to **₹92 crore** in 2020. This indicates that smuggling operations are on the rise, with **Bangladesh** and

Myanmar acting as key entry points for fake currency into India.

India's Multi-Pronged Response

To fight this threat, India has adopted a multi-layered strategy:

- **Tougher Laws:** The **Unlawful Activities (Prevention) Act (UAPA), 1967**, was amended to classify the production or smuggling of fake currency as a **terrorist act**. It is also a serious crime under the **Indian Penal Code**.
- **RBI Security Measures:** The **Reserve Bank of India (RBI)** continuously upgrades banknotes with advanced security features like watermarks, security threads, and latent images to make them harder to copy.
- **National and International Cooperation:** The **FICN Coordination Group** ensures intelligence sharing between different Indian agencies. The **National Investigation Agency (NIA)** specifically investigates terror funding links, and India actively cooperates with neighboring countries like **Nepal** and **Bangladesh** to stop cross-border smuggling.

2.2. Linkage between Organized Crime and Terrorism

Both **organized crime** and **terrorism** are **intertwined** and **mutually interchangeable** due to their **similarities**. Some **terrorist organizations** are funded by **organized crime**, while certain **criminal organizations** use their **financial power** to pursue **political ambitions** through **terrorism.**

Similarities between Organized Crime and Terrorism

- **Similar Member Profiles**: Both organized crime and terrorism recruit individuals from marginalized social groups, often attracted by **excitement**, **risk-taking**, and a disdain for **social norms**.
- **Punishable by Law**: Both entities engage in **illegal activities**, often utilizing **advanced technology** for high-tech crimes, and are subject to legal **punishment**.
- **Strict Discipline and Planning**: Both groups exhibit **careful planning**, **rigorous discipline**, and an internal system of **punishment** to maintain **order** and **obedience** within their ranks.
- **Secrecy, Violence, and Interdependence**: Both rely on **secrecy**, use **violence** for their goals, and are **interconnected**, with organized crime often financing terrorist activities and vice versa.

Differences between Organized Crime and Terrorism

Aspect	Terrorism	Organized Crime
Motivation	**Ideological and Political Goals**: Terrorists act out of a desire to achieve political, ideological, or religious goals. Example **Al-Qaeda**, **ISIS**, **Boko Haram**, and **Taliban**	**Economic Gain**: Organized crime groups are motivated by the pursuit of personal **financial profit**. Example **Italian Mafia**, **Russian Mob**, **Yakuza**
Visibility	**High Visibility**: Terrorists openly declare their intentions and claim responsibility for attacks to garner attention, spread their message, and gain support from sympathetic populations. • Terrorists usually claim responsibility for their attacks	**Low Visibility**: Organized crime groups operate **in the shadows**, focusing on secrecy to avoid detection by authorities. • Members of organized crime groups rarely, if ever, claim responsibility for criminal activities.

Student Notes:

Relationship with the State	**Confrontational**: Terrorists actively challenge the state's authority. They aim to **overthrow** or **transform** the government, often through violent means.	**Covert and Corruptive**: Organized crime groups may engage with the state through **bribery**, **corruption**, and **infiltration**.
Methods	**Violence and Terror**: Terrorists often use **high-profile violent actions** (bombings, kidnappings, assassinations) to disrupt society and instill fear.	**Criminal Activities**: Organized crime groups focus on **illicit economic activities** like drug trafficking, human trafficking, money laundering, and extortion.
Relationship with Society	**Public Awareness**: Terrorist groups aim to **gain support** from a segment of the population for their cause.	**Invisible to the Public**: They use their power to manipulate local communities, but their primary focus is on **profit and secrecy**, not public support or recognition.

2.2.1. The Crime-Terror Nexus

"Terrorism is funded by laundering; Anti-money Laundering is counter-terrorism" - UN Security Council

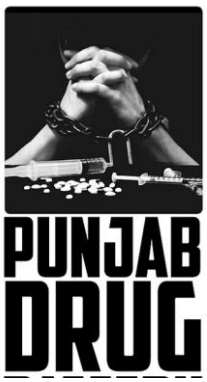
While **Organized Crime** fundamentally seeks **profit** and **Terrorism** is driven by **ideology**, these two threats are increasingly connected in a dangerous partnership. They cooperate, share methods, and often rely on each other to survive and thrive.

1. **Terrorist Financing**

Terror groups often run their own criminal enterprises to generate revenue. Classic examples include the financing of the **Taliban** through **opium** production. On the other hand, money laundering is often described as the **"lifeblood of terrorism,"** providing terrorist organizations with the necessary financial resources to sustain their operations. These funds are used for:

- **Procuring weapons and explosives**
- **Maintaining training camps**
- **Paying cadres and recruiting new members**
- **Carrying out propaganda activities**

As confirmed by India's **Financial Intelligence Unit (FIU)** and global bodies like the **FATF**, groups like **Lashkar-e-Taiba** funnel illicit money through legitimate businesses, NGOs, and informal channels like **hawala**.



Punjab's Double Edged Crisis: Drugs & Separatism

Punjab battles a severe **drug crisis** affecting its **youth**. The **Golden Crescent** fuels this, with **Pakistan-linked cartels** trafficking heroin via **drones** into Punjab.

These illicit funds directly finance **Khalistani separatist groups**.

Rebels or Cartels? The Rise of Criminalized Insurgencies

The **UNODC** highlights the trend of **"Criminalized Insurgencies,"** where rebel groups begin to act more like powerful criminal cartels.

A key example is **Myanmar's Arakan Army**, which relies on **methamphetamine trafficking** for as much as **60%** of its revenue. This deep involvement in **illicit trade** blurs the line between their **political** goals and their **profit motives**, creating dangerous hybrid groups where crime directly funds their military ambitions.

Student Notes:

2. Narco-Terrorism

Narco-terrorism is a vicious cycle where **drug traffickers** and **terrorists** collaborate for mutual benefit:

- **Drug Trafficking Finances Terror**: Insurgent and terrorist groups generate substantial funds by controlling and taxing narcotics cultivation and trafficking.
- **Terror Protects Drug Routes**: Terrorist groups use their military strength to protect drug routes from law enforcement, ensuring the smooth flow of contraband. India's proximity to the **"Golden Crescent"** and **"Golden Triangle"** makes it highly vulnerable to this threat.

3. The Illegal Arms Trade

The **illegal arms trade** is a critical enabler for terror groups in **India** and worldwide.

- Weapons are acquired through clandestine networks that exploit porous borders and corrupt officials, often using the same smuggling routes as narcotics traffickers, especially in **Northeast India** and **Jammu & Kashmir**.
- These illicit arms directly strengthen groups like **Lashkar-e-Taiba** and **ULFA**, allowing them to carry out attacks and prolong internal conflicts.

4. Intellectual Property Crime

A surprisingly massive source of funding comes from **Intellectual Property Crime (IPC)**—the illicit trade in counterfeit goods.

- This black market, sometimes considered larger than the global drug trade, is a key source of funds for groups like **Al-Qaeda**.
- For example, in **2016**, terrorist groups in North Africa generated an estimated **$1 billion** from the contraband tobacco trade alone.

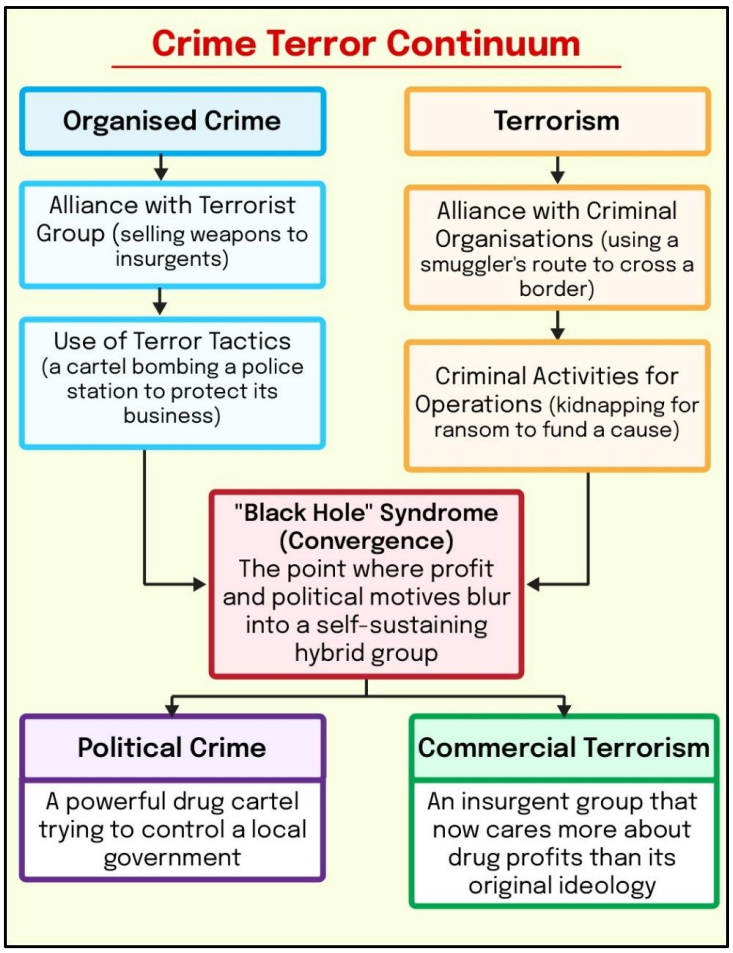
5. Human Trafficking as a Tool of Terror

Recently, groups like **ISIS** and **Boko Haram** have used **human trafficking** not just for profit but also as a strategic tool. They use it to increase their manpower by recruiting **child soldiers** and for sexual abuse and intimidation, treating people like commodities on the black market.

Student Notes:

2.2.2. Why the Linkage Matters

The **linkage** between **organized crime** and **terrorism** creates a **"force multiplier"** for both, amplifying their **threats** to national security:



- **Escalation of Threats**: Their **cooperation** strengthens both groups' **capacity** to inflict damage, creating a **bigger** and **more dangerous** threat.
- **Undermining State Sovereignty & Rule of Law**: The **criminal-political nexus** erodes **economic sovereignty**, fosters **corruption**, and **weakens the state**.
- **Challenges to National and International Security**: These linkages, which **transcend borders**, require a **global response** to effectively tackle this **cross-border** threat.

2.2.3. Crime- Terror Nexus in the Indian Context

Organized crime and terrorism in India are **closely linked** through illegal activities such as:

- **Drug trafficking**
- **Arms smuggling**
- **Human trafficking**
- **Money laundering**

Key Areas of Convergence in India

The nexus between organized crime and terrorism is evident across multiple regions and sectors in India. Some critical areas where these threats converge include:

Region	Key Issues	Details
Jammu & Kashmir	**State-sponsored Terrorism**: Supported by Pakistan's ISI.	Militant groups backed by Pakistan's intelligence agency.
	Funding: Primarily from Pakistan and Gulf countries, facilitated through Hawala transactions.	Terrorist groups receive financial support from foreign sources.
	Narco-terrorism: Narcotics account for about 15% of militant group finances.	Drug trafficking contributes to the funding of terrorism.

Student Notes:

Punjab	**Drug Crisis**: Exacerbated by proximity to Pakistan, especially near the Ferozepur sector.	Punjab faces a severe drug trafficking issue due to its location.
	Drug Trafficking: Heroin is used by militant groups to finance operations.	Militant operations in Punjab are funded by the trade of heroin.
	Drones: Increased use of drones to smuggle arms, ammunition, and drugs.	Drones complicate border security, enhancing illegal activities.
Northeast India	**Golden Triangle**: Hub for drug trafficking, exploited by insurgent groups for illicit goods.	The region is a key point in the global drug trade.
	Transnational Networks: Facilitated by networks from Myanmar and Cambodia for drugs, arms, and human trafficking.	International syndicates are involved in smuggling activities.
	Parallel Governments: Insurgent groups establish parallel governments funded by extortion.	Parallel governments funded by illegal means undermine state control.
Coastal Security	**Vulnerability**: Prone to smuggling, including narcotics, arms, and explosives.	The coastline faces challenges in controlling illegal activities.
	Post-26/11 Security: Focus on improving maritime security with better surveillance and intelligence gathering.	Enhanced maritime security since the 26/11 Mumbai attacks.
Cyber Domain	**Cyber-Crime**: India is the second-most-attacked nation in the Asia-Pacific region (2020).	A growing number of cyber-attacks targeting various sectors.
	Technology-Terrorism Nexus: Use of digital platforms for communication, recruitment, and fundraising.	Terrorist groups exploit modern technologies like virtual assets and drones for financing and operations.

2.2.4. Fighting Organized Crime: Initiatives, Challenges, and the Way Forward

This section outlines the key steps taken by India and the global community to fight organized crime, the major hurdles they face, and the recommended path forward.

Indian Initiatives Against Organized Crime

India has launched several targeted efforts to combat different forms of organized crime:

- **Combating Human Trafficking:** The **Ministry of Home Affairs (MHA)** has set up an **Anti-Trafficking Nodal Cell**. The government also funds NGO-run shelters through the **Ujjawala** and **Swadhar** programs. The proposed **Trafficking of Persons Bill, 2021**, aims to create special courts and rehabilitation committees to strengthen these efforts further.

Student Notes:

- **Tackling Drug Trafficking:** India uses laws like the **Narcotics Drugs and Psychotropic Substances Act (NDPS Act), 1985**, to fight the drug menace. As a signatory to all three **UN Conventions** on drugs, India cooperates with global bodies like the **UNODC**. A recent success was **Operation Dhvast (2023)**, where the **NIA** busted a major terrorist-gangster-drug trafficking nexus.
- **State-Level Legislation:** While India lacks a single national law on organized crime, state-level laws like the **Maharashtra Control of Organized Crime Act (MCOCA), 1999**, have been very effective in curbing crime syndicates in Maharashtra and Delhi.

Global Initiatives

The primary international tool is the **United Nations Convention against Transnational Organized Crime (UNTOC)**.

- This convention commits countries to create domestic laws against organized crime, money laundering, and corruption.
- It is supplemented by three specific **Protocols** targeting **Trafficking in Persons** (especially women and children), **Smuggling of Migrants**, and the **Trafficking in Firearms**.

The Way Forward: What More Needs to be Done

To effectively combat these evolving threats, several steps are needed:

- **Improved Coordination:** Set up a **National Level body** to act as a central hub for intelligence on organized crime.
- **Enhanced International Cooperation:** Focus on **speedy extradition** of fugitive criminals and strengthen the role of **Interpol**.
- **Capacity Building and Awareness:** Better training for police and intelligence agencies, effective implementation of strong laws like **MCOCA**, and raising **public awareness** to involve citizens in prevention.

As former UN Secretary-General **Ban Ki-moon** stressed, the response to these interconnected threats must be coordinated and global.

UNIT 5: SECURITY CHALLENGES AND THEIR MANAGEMENT IN BORDER AREAS

Student Notes:

"Border management is not just about fences and guns; it is about creating a seamless interface between security and development." – K. Santhanam, IDSA

Previous Years Question

- **(2024)** India has a long and troubled border with **China and Pakistan** fraught with contentious issues. Examine the conflicting issues and security challenges along the border. Also give out the development being undertaken in these areas under the **Border Area Development Programme (BADP)** and **Border Infrastructure and Management (BIM) Scheme**. (15m, 250w)
- **(2023)** The use of **unmanned aerial vehicles (UAVs)** by our adversaries across the borders to ferry arms/ammunitions, drugs, etc., is a serious threat to internal security. Comment on the measures being taken to tackle this threat. (150 words/10m)
- **(2022)** What are the **maritime security challenges** in India? Discuss the organisational, technical and procedural initiatives taken to improve maritime security.(10 marks)
- **(2021)** How is the **S-400 air defence system** technically superior to any other system presently available in the world? (150 words)
- **(2020)** For effective **border area management**, discuss the steps required to be taken to deny local support to militants and also suggest ways to manage favourable perception among locals.
- **(2020)** Analyze internal security threats and **transborder crimes** along Myanmar, Bangladesh and Pakistan borders including Line of Control (LoC). Also discuss the role played by various security forces in this regard.
- **(2019)** Cross-border movement of insurgents is only one of the several security challenges facing the policing of the border in North-East India. Examine the various challenges currently emanating across the **India-Myanmar border**. Also, discuss the steps to counter the challenges.
- **(2017)** The **north-eastern region** of India has been infested with insurgency for a very long time. Analyze the major reasons for the survival of armed insurgency in this region.
- **(2016) Border management** is a complex task due to difficult terrain and hostile relations with some countries. Elucidate the challenges and strategies for effective border management.
- **(2014) International civil aviation laws** provide all countries complete and exclusive sovereignty over the airspace above the territory. What do you understand by airspace? What are the implications of these laws on the space above this airspace? Discuss the challenges which this poses and suggests ways to contain the threat.
- **(2014)** How does illegal **transborder migration** pose a threat to India's security? Discuss the strategies to curb this, and bring out the factors which give impetus to such migration.
- **(2014)** In 2012, the longitudinal marking of the high-risk areas for **piracy** was moved from 65° East to 78° East in the Arabian Sea by the International Maritime Organisation. What impact does this have on India's maritime security concerns?
- **(2013)** How far are India's internal security challenges linked with **border management**, particularly in view of the long porous borders with most countries of South Asia and Myanmar?

1. Foundations of Border Management

Student Notes:

Border management is a **multifaceted and integrated strategy** that goes beyond purely defensive measures. It involves **coordinated actions** across various sectors, including **security, administration, diplomacy, intelligence, legal, and economic agencies**.

Key Objectives:

- **Securing the Frontiers**: The primary aim is to protect the nation from hostile threats like infiltration, cross-border terrorism, smuggling, and illegal migration.
- **Facilitating Legitimate Trade and Transit**: A crucial aspect is enabling legal cross-border trade and travel, promoting economic growth, and maintaining positive relations with neighboring countries.

This approach recognizes that border security cannot operate in isolation. A balanced strategy is needed that considers both **security needs** and the **socio-economic well-being** of border populations, while also ensuring efficient and legal interactions across borders.

India's Frontiers: An Overview

A Statistical Look

India's borders and **geographical features** present a significant challenge for national security management:

- **Land Border**: India shares a **15,106.7 km** long land border with seven countries, which requires constant vigilance and efficient border management systems.
- **Coastline**: With a coastline stretching **7,516.6 km**, including its island territories, India faces various **maritime security threats** that require specialized naval and coastal security measures.

Radcliffe Line: A Legacy of Conflict

The **Radcliffe Line (1947)**, an **artificially drawn border** between India and Pakistan, was hastily demarcated without local consideration. This flawed partition inherently **ignited perpetual India-Pakistan disputes**.

Its arbitrary nature fueled **mass migration, violence**, and unresolved territorial claims, most notably **Kashmir**. This historical demarcation remains a fundamental source of enduring hostility between the two nations.

Student Notes:

Characteristics of India's Neighbourhood

India's strategic location is defined by its unique and often challenging geopolitical environment:

- **Diversity**: The region is marked by significant **cultural, political, and economic** diversity, which presents both opportunities and challenges for cooperation.
- **Asymmetry**: India is much larger in terms of population and size compared to most of its neighbors, which creates a **power imbalance** and complex diplomatic relationships.
- **Political Instability**: While India has solidified its democratic structure, many of its neighbors continue to face **political instability** and incomplete nation-building, leading to **spillover effects** on India.
- **Least Integrated Region**: Despite many shared interests, **South Asia remains one of the world's least economically integrated regions**, hindering regional stability and growth.
- **Influence of External Powers**: The region is also an arena for the **influence and competition of major external powers**, which adds layers of complexity to India's security challenges.

2. Key Challenges in Indian Border Management

"Borders are not just lines on maps but complex interfaces of security, economy, and human dignity." – EU Black Sea Strategy, 2025

India's border management is **affected by** a combination of **geographical**, **political, administrative,** and **socio-economic challenges,** many of which are common across its vast and diverse frontiers.

Siachen: Nature's Ultimate Border Test

The **Himalayan glaciers**, notably **Siachen**, present extreme **geographical challenges** for border management. **Temperatures plunging to -60°C** create immense **logistical nightmares** for troops.

This harsh environment tragically causes **more casualties from weather** (avalanches, frostbite) than from combat, highlighting the overwhelming natural dangers faced in securing these high-altitude **borders**.

1. **Geographical Challenges: Difficult and Diverse Terrains**

   India's borders pass through some of the most **difficult terrains** in **the world**, making their **security particularly challenging:**

   - **Mountains**: The high-altitude Himalayan ranges along the border with China.
   - **Deserts**: The arid Thar Desert in Rajasthan.
   - **Marshes**: The swampy, riverine terrain of the Rann of Kutch in Gujarat.
   - **Riverine Belts**: Shifting river courses along the Indo-Bangladesh border make fencing and permanent demarcation difficult.
   - **Dense Forests**: The thick jungles along the Indo-Myanmar border offer natural cover for insurgents and smugglers, contributing to porous borders and easy infiltration.

Student Notes:

China's Cartographic Warfare

China is continuing its **cartographic aggression**. In a provocative move in **May 2025**, Beijing released new "**standard maps**" that falsely claim India's **Arunachal Pradesh** and the entire **South China Sea** as its own territory. This is a modern take on historical **"cartographic colonialism."**

In response, **India strongly counters** these baseless claims. India is firmly using its **existing stringent laws**, which make it a criminal offense to depict the country's borders incorrectly.

2. **Political & Historical Challenges: Un-demarcated and Disputed Borders**

India's borders are often a legacy of **colonial-era decisions,** which created boundaries that are not always aligned with natural features:

- **Disputed Borders**: India has unresolved disputes with Pakistan and China. The lack of a mutually agreed-upon Line of Control (LoC) with Pakistan and Line of Actual Control (LAC) with China leads to persistent tensions and military standoffs.
- **Un-demarcated Sections**: Even with friendly neighbors, some sections of the border remain un-demarcated, contributing to disagreements and potential friction.

Centralized vs. Fragmented Border Security

The **EU's Frontex Agency** showcases a model of **centralized border force coordination** across 27 nations, leveraging **interoperable technology**. This approach streamlines operations and enhances security.

In contrast, India's border management, characterized by agencies like **BSF, ITBP, and SSB**, suffers from **fragmentation**. This highlights persistent **coordination gaps**, impacting efficiency and comprehensive border control.

3. **Administrative Challenges: The Problem of Multiplicity of Forces**

The presence of **multiple forces** along India's borders **creates coordination and management issues:**

- **Fragmented Command**: For example, the border with China is managed by various forces, including the Indo-Tibetan Border Police (ITBP), Indian Army, and the Special Frontier Force, which leads to fragmented command and control.
- **"One Border, One Force" Principle**: While the government has adopted this policy to streamline border management, its implementation remains incomplete.

4. **Socio-Economic Challenges: Alienation of Border Populations**

The border areas of India often suffer from underdevelopment, which contributes to socio-economic challenges:

Border Vulnerabilities:

Punjab Border: In **Punjab**, **"Drones & Discontent" (2025)** highlights **WHAM (Winning Hearts and Mind) gaps**. Farmers near the **International Border (IB)** lack **tech jobs**, making them susceptible to **smuggling networks** offering lucrative **drone-pilot roles**, fueling illicit activities.

Myanmar Border: Along the **Myanmar border**, **Chin refugees** fleeing junta violence (2024) reveal another WHAM challenge. **Underdevelopment** in these regions is exploited, aiding **insurgent recruitment** (e.g., **NSCN-K**), exacerbating regional instability.

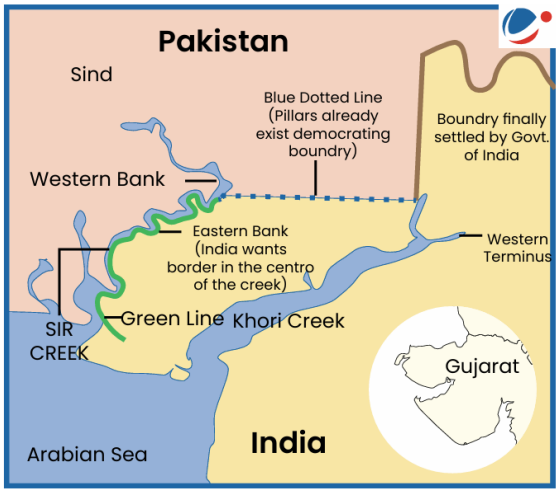
Student Notes:

- **Psychological Alienation**: These areas lack basic infrastructure and livelihood opportunities, leading to a sense of alienation among local populations.
- **Security Implications**: **Discontented communities** in border areas are vulnerable to exploitation by **hostile state and non-state actors**, who use them for intelligence gathering, logistics, and shelter. Integrating these communities and making them stakeholders in border security is a critical element of effective border management.

3. Border-by-Border Analysis of Security Challenges

3.1. Western Frontier: The India-Pakistan Border

India's **border** with **Pakistan**, spanning **3,323 km**, is one of the most heavily militarized and volatile borders globally. It is a composite of different segments, each with unique security dynamics shaped by geography, political relations, and history.



Nature of the Border

The India-Pakistan border can be divided into three distinct sections:

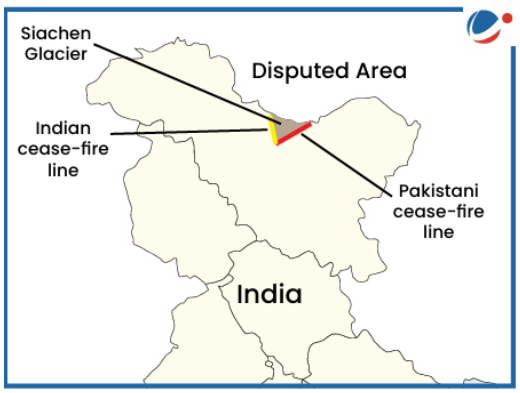
- **International Border (IB)**: Running from Gujarat to Jammu, this boundary is recognized internationally but faces constant infiltration attempts and smuggling activities.
- **Line of Control (LoC)**: This 776 km de facto boundary emerged after the 1948 and 1971 wars. It is not internationally recognized but is a frequent site of military confrontations and ceasefire violations.
- **Actual Ground Position Line (AGPL)**: A 110 km line in the Siachen Glacier region, marking the positions held by Indian and Pakistani troops.

KAVACH laser walls

"KAVACH laser walls" are an **authentic, indigenous technology** deployed along a **198 km stretch** of the **India-Pakistan border in Jammu**. This advanced system utilizes **invisible infrared beams** for intrusion detection.

Upon detecting breaches, **KAVACH** immediately relays **real-time alerts** to **BSF posts**. This enhances border security, enabling rapid response to **intrusions** and bolstering the overall vigilance in challenging terrains.

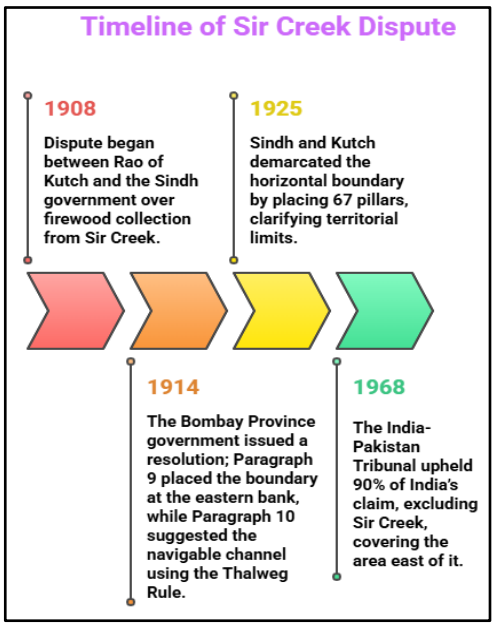
Key Security Challenges



- **Cross-Border Infiltration of Terrorists**: The difficult terrain and cover of cross-border firing are exploited by Pakistan's ISI to send well-trained terrorists into India particularly in Jammu & Kashmir
- **Frequent Ceasefire Violations and Military Standoffs**: The LoC is frequently marked by ceasefire violations, which are often strategic, used to facilitate infiltration attempts and keep the border tension-filled.
- **Transborder Smuggling of Narcotics and Arms**: The western frontier, especially in Punjab and Rajasthan, is a significant route for smuggling narcotics (mainly heroin) from the "Golden Crescent" region and arms used by terrorists and criminal syndicates operating within India.

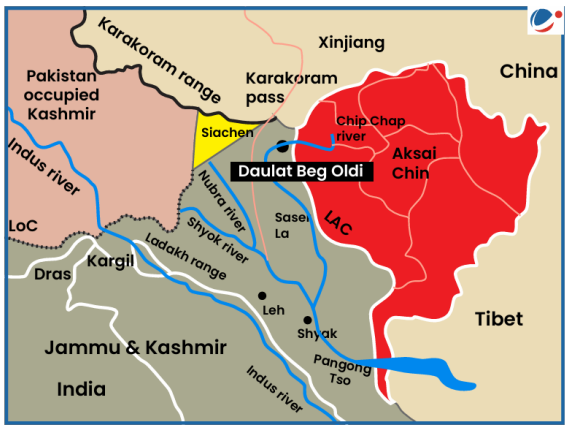
Student Notes:

- **Unresolved Territorial Disputes**:
  - **Siachen Glacier**: The **world's highest battlefield**, strategically important for India, remains a contested area. India pre-emptively occupied it in 1984 to counter Pakistan's moves, safeguarding Ladakh and the Leh-Srinagar highway from Pakistani control and ensuring security against Chinese territorial ambitions.
  - **Sir Creek**: A **96-km tidal estuary in the marshy Rann of Kutch**, the dispute centers around differing interpretations of a 1914 map.
    - > While India follows the **Thalweg doctrine** (boundary should follow the deepest part of the main navigable channel), Pakistan claims the entire creek.
    - > The unresolved dispute facilitates smuggling and terrorism, as demonstrated in the 26/11 Mumbai attacks, where terrorists used a sea route near Sir Creek to infiltrate India.



3.2. The Northern Frontier: Managing the India-China Border

The **India-China border** spans 3,488 km and is marked by a fundamental disagreement over its alignment, making it a zone of strategic competition and military tension.



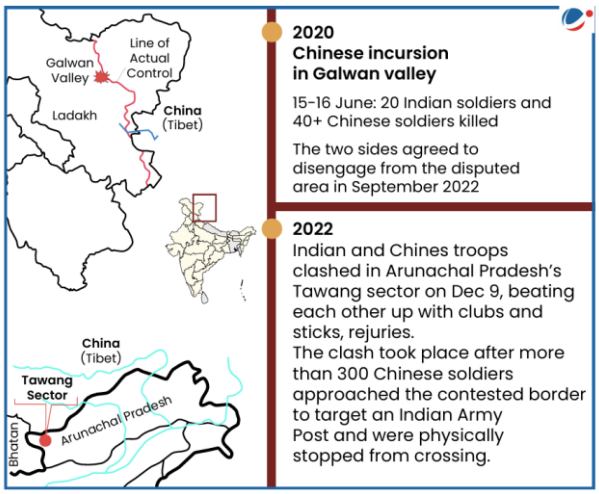
Nature of the Border: The Contested Line of Actual Control (LAC)

Unlike the **Line of Control (LoC)** with Pakistan, the **Line of Actual Control (LAC)** with China is not mutually agreed upon and remains **un-demarcated** over large stretches. Both countries have differing perceptions of the LAC, which often leads to overlapping claims and face-offs when patrols from either side assert their presence. The border is divided into three sectors:

- **Western Sector (Ladakh)**
- **Middle Sector (Himachal Pradesh, Uttarakhand)**
- **Eastern Sector (Sikkim, Arunachal Pradesh)**

Key Security Challenges

- **Military Transgressions and Standoffs:** Frequent transgressions by the **People's Liberation Army (PLA)** result from differing perceptions of the LAC. These provocations are often deliberate, testing India's resolve and asserting Chinese claims. Notable incidents include:



Student Notes:

- **Doklam (2017)**: Indian troops blocked the PLA from constructing a road on the disputed Doklam plateau, located at the India-Bhutan-China tri-junction. This road posed a threat to India's **Siliguri Corridor** (also called the "Chicken's Neck").
- **Galwan Valley (2020)**: A violent clash between Indian and Chinese troops in Ladakh led to casualties on both sides. This was the first major clash in decades and marked a significant deterioration in bilateral relations.

Doklam: Grey-Zone Challenge

The **Doklam standoff (2017)** exemplifies **Grey-Zone warfare**. **China's road construction** in disputed Bhutanese territory **challenged India's strategic dominance** near the Siliguri Corridor, a critical vulnerability.

Resolved after 73 days, the crisis ended through **diplomatic coercion** and mutual disengagement. This case highlighted how nations assert claims and test resolve without escalating to full-scale military conflict.

- **China's Use of "Grey-Zone Warfare" and "Salami Slicing"**
  - China employs **Grey-Zone Warfare** tactics to achieve strategic objectives without direct conflict.
  - **Salami slicing** refers to small, incremental changes made to the status quo that are minor to provoke a major military response, but over time, they accumulate and alter the strategic landscape in China's favor. This tactic is evident in China's continuous construction of infrastructure like posts and roads along the LAC.
- **Rapid Infrastructure Development and Strategic Asymmetry:** China's rapid development of infrastructure along the LAC in Tibet—including roads, railways, and airfields—has created a **strategic asymmetry**. This infrastructure enables the **PLA** to quickly mobilize troops and deploy equipment, putting India at a significant military disadvantage.
- **The Strategic Implications of the China-Pakistan Economic Corridor (CPEC):** The **China-Pakistan Economic Corridor (CPEC)**, a key component of China's **Belt and Road Initiative**, passes through **Pakistan-Occupied Kashmir (PoK)**, which India claims as its own territory. This project undermines India's sovereignty and territorial integrity.

3.3. The Eastern Frontiers - Managing Borders with Bangladesh and Myanmar

India's eastern borders are defined by **diverse geographical features, ethnic continuities** across borders, and a **history of insurgency** and **illegal migration**, presenting unique challenges.

Rohingya Muslims Issue in India – Bangladesh Connection

Rohingya Muslims, fleeing violence in **Myanmar** since 2012, initially sought refuge in **Bangladesh** before crossing illegally into **India**. Their influx into **West Bengal**, **Assam**, and **Jammu** raises concerns over **illegal immigration**, **security risks** and resource strain.

The India-Bangladesh Border

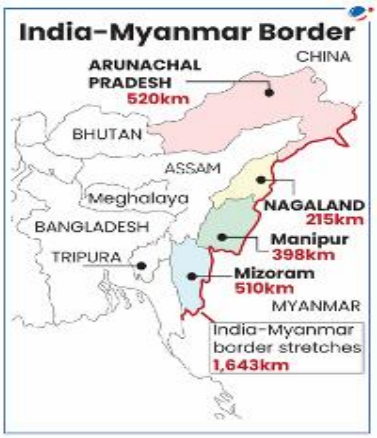
India balances **security** with **humanitarian obligations** while coordinating with **Bangladesh** on **cross-border movement** and **deportations**.

- **Primary Challenge - Illegal Migration:** The 4,096 km India-Bangladesh border is the longest India

shares with any neighbor. The **primary security concern** is the **large-scale illegal migration** from Bangladesh, which has l**ed to demographic changes** in states like Assam and West Bengal. This migration **fuels social** and **ethnic tensions,** increasing pressure on local resources and infrastructure.

- **Other Challenges:** The border is also notorious for **cattle smuggling**, with an estimated one lakh cattle being smuggled annually, leading to financial losses and violence. Other issues include **human trafficking** and the smuggling of **contraband**.
- **Successes in Management- India-Bangladesh Land Boundary Agreement (2015):** Despite challenges, the **India-Bangladesh Land Boundary Agreement (2015)** effectively **resolved** the complex **enclave issue** along their 4096 km border. This **historic accord** formally integrated territories, demonstrating successful **diplomatic engagement**.

Crucially, the agreement directly **benefited over 52,000 people**, providing national identity and services. It stands as a powerful **model for peaceful dispute resolution**, significantly fostering stronger bilateral ties.



The India-Myanmar Border

- **Primary Challenge - A Haven for Insurgents:** The 1,643 km border with Myanmar passes through **rugged terrain** and dense forests, making it a security concern.
  - The **border's porosity** and the **ethnic ties** across it have **allowed insurgent groups** from North-East India (such as NSCN factions) to set up safe havens, training camps, and operational bases in Myanmar.
- **Other Challenges:** The border's proximity to the **Golden Triangle** makes it a major route for **drug trafficking** (especially **heroin** and **methamphetamine**) and arms smuggling, which finances insurgent activities.
- **The Free Movement Regime (FMR):** The Free Movement Regime (FMR) **allowed border populations to travel up to 16 km** across the border without a visa.

While it facilitated social and trade ties, the regime was misused by insurgents for **infiltration** and **smuggling**, contributing to illegal immigration. **In 2024**, the Indian government decided to scrap the FMR and fence the entire border to curb these issues.

Securing the Porous Frontier (2024-25)

India's **India-Myanmar border policy** underwent a significant **shift in 2024-2025**. Driven by security concerns like **insurgency** and **drug trafficking**, the **Free Movement Regime (FMR)** was **scrapped**.

Simultaneously, India is embarking on **extensive border fencing** along the 1,643 km frontier. New rules, effective December 2024, mandate **biometric border passes** for tribal communities, tightening control and enhancing **real-time vigilance** through technology.

3.4. Open Borders - Managing Frontiers with Nepal and Bhutan

India shares open, unfenced borders with **Nepal** (1,751 km) and **Bhutan** (699 km), governed by **Friendship Treaties** that allow for the free movement of people. While these arrangements foster close relations, they also present unique security challenges.

Nepal: A Gold Smuggling Conduit

Nepal serves as an **authentic and significant transit point for gold smuggling into India**, largely exploiting the **porous open border**. This long-standing issue allows illicit gold, often from China or the Middle East, to circumvent stricter Indian security measures.

Key Security Challenges

- **Misuse as a Transit Route:** A major security concern is the misuse of these open borders as a transit route for **terrorists**, **criminals**, and **third-country nationals**. **Pakistan's ISI** often

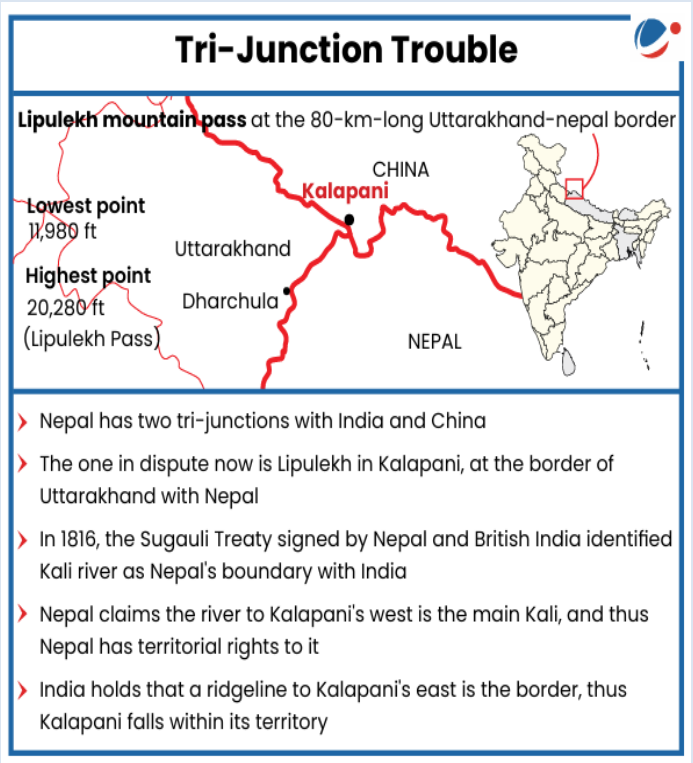
Student Notes:

facilitates the movement of **terrorists**, **Fake Indian Currency Notes (FICN)**, and **narcotics** across these borders, using them as entry points into India.

- **Smuggling of Goods:** The borders are also exploited for the **smuggling of goods**, including **Chinese-made electronics** and **forest products**, which bypass customs and regulatory checks, causing significant revenue losses.
- **Emerging Border Disputes:** While the borders remain largely peaceful, **border disputes** have arisen, creating diplomatic friction. A prominent example is the **Kalapani territorial dispute** with Nepal, where Nepal claims areas that India considers part of its territory in **Uttarakhand**. This dispute has led to tensions between the two countries.

Recent Border Dispute with Nepal

Nepal recently released a new political map claiming **Kalapani**, **Limpiyadhura**, and **Lipulekh**—strategically important regions of **Uttarakhand**, India, as part of its territory, raising concerns over the border dispute.



Nepal's Viewpoint

Nepal bases its claim on the **1816 Treaty of Sugauli**, which set the **Kali River** (Mahakali in Nepal) as the **north-western border**. Nepal argues that the **source of the Kali River** lies near **Limpiyadhura**, so it claims the region, including **Kalapani** and **Lipulekh**, lies to its east.

India's Viewpoint

India asserts the border starts at **Kalapani**, where the **Kali River** originates. India claims **Kalapani** has been part of **Pithoragarh district** in **Uttarakhand** since the 19th century and has been under Indian control since the **1950s**, with infrastructure, administration, and **military presence**.

China's Recognition

In **2015**, **China** recognized India's sovereignty over **Kalapani** and agreed to expand **trade** through the **Lipulekh pass**, further strengthening India's claim.

3.5. Open Borders - Managing Frontiers with Sri Lanka

Sri Lanka shares a **maritime border with India** and is a very important country **strategically placed** in the **Indian ocean** for India's security.

Key security Challenges along the border Sri Lankan Border:

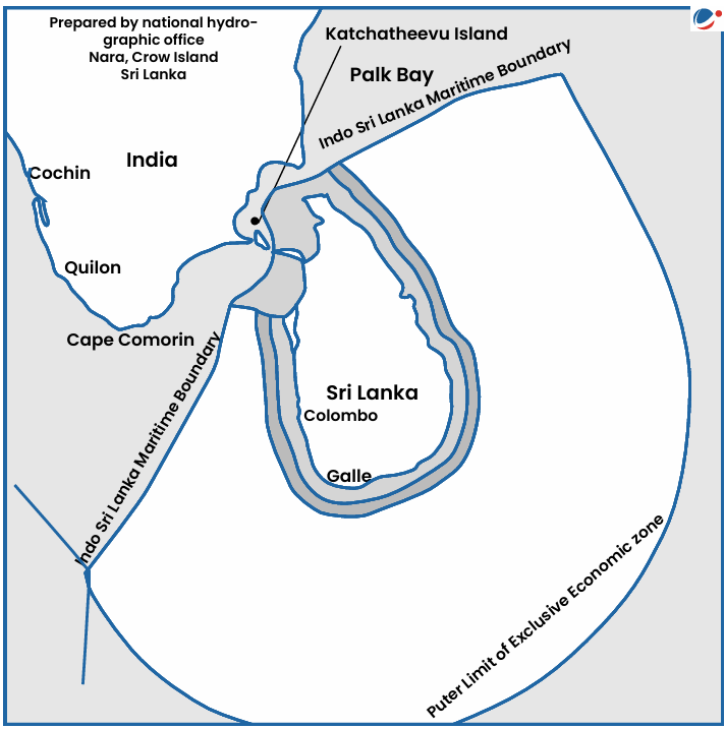
- **Katchatheevu Island : India ceded the uninhabited island to its southern neighbour in 1974**

Black Sea's Three-Pronged Shield

The **EU's Black Sea Strategy** integrates **security**, **economic prosperity**, and **environmental resilience** through a **"Three-Pillar Framework"**.

This approach stabilizes the region by addressing **military**, **trade**, and **climate** challenges synergistically, promoting **sustainable growth** and combating **hybrid threats**. **India** can apply a similar strategy to the **Indo-Sri Lankan** issue, focusing on **connectivity**, **security**, and **climate resilience**.

under a conditional accord. However, **Indian fishermen** considered it to be their **traditional fishing area and want Katchatheevu** to be used as fishing grounds for India as well.



- **Fishermen issue:** The **Fishermen Issue** revolves around **Indian fishermen** frequently **trespassing** into **Sri Lankan waters**, not due to an unsettled maritime boundary, but because of the refusal of Indian fishermen to acknowledge the maritime boundary between **India** and **Sri Lanka**, especially in the **Palk Bay**. Sri Lanka has introduced **tougher laws** banning **bottom trawling** and imposing **heavy fines** on **foreign vessels** that **trespass** into its waters.

4. India's Comprehensive Border Management Strategy

To address the multifaceted challenges along its borders, India has implemented a **comprehensive border management strategy**. This integrates **policy**, **security force deployment**, **developmental initiatives**, and **technology** to ensure both security and socio-economic development.

1. **Policy and Administrative Framework**
   - **The Principle of "One Border, One Force":** India has adopted the **"One Border, One Force"** principle to improve accountability, coordination, and specialization in border management. The idea is to assign the security of each border to a single force. However, the implementation faces challenges, especially along the **China border**, where multiple forces currently operate.
2. **Role of Border Guarding Forces (BGFs)**
   - **Border Security Force (BSF)**: Manages the borders with **Pakistan** and **Bangladesh**.
   - **Indo-Tibetan Border Police (ITBP)**: Secures the high-altitude border with **China**.
   - **Sashastra Seema Bal (SSB)**: Guards the open borders with **Nepal** and **Bhutan**.
   - **Assam Rifles**: Manages the **Indo-Myanmar border** and conducts **counter-insurgency** operations in the **North-East**.

Madhukar Gupta Committee

- It was tasked give recommendations for strengthening border protection and addressing the issue of gaps and vulnerability in border fencing along India-Pakistan Border.
- It was constituted three months after the terror attack on Pathankot IAF base in January 2016 by Jaish-e-Mohammed (JeM) terrorists from Pakistan
- Recommended the use of scientific technology in border management. For example, use of laser fencing, ground sensors and thermal imaging where physical fencing is not feasible due to difficult terrain.
- It gave separate recommendations for four states as each of them has different topography and problems.

Student Notes:

3. **Developmental Initiatives in Border Areas**

- **The Border Area Development Programme (BADP):** A centrally sponsored scheme focused on improving infrastructure and socio-economic conditions in **remote border areas**. It emphasizes sectors like **health**, **education**, **connectivity**, and **agriculture**, helping reduce the sense of alienation among border populations.
- **The Vibrant Villages Programme (2022):** Launched to enhance the development of select villages along the **northern border with China**. The programme aims to improve **living standards** and encourage **population retention**, thereby bolstering both security and socio-economic stability in these strategically important regions.

4. **Technological and Infrastructural Upgradation**

- **Comprehensive Integrated Border Management System (CIBMS):**
  - The **CIBMS** is a vital initiative to create a **"smart fence"** that combines technology with human resources.
  - It includes the **Project BOLD-QIT (Border Electronically Dominated QRT Interception Technique)** for the **riverine border with Bangladesh**, designed to enhance security and interception techniques.
- **Use of Surveillance Technology:**
  - **Thermal imagers** and **night-vision devices** for round-the-clock surveillance.
  - **Battlefield surveillance radars** and **underground monitoring sensors** to detect hidden threats.
  - **Laser barriers** and **Unmanned Aerial Vehicles (UAVs)** for continuous monitoring.
- **Role of Space Technology**
  - India utilizes **space technology** for comprehensive border management. Satellites like the **Cartosat series** provide high-resolution imagery for **real-time monitoring** and **intelligence gathering**, greatly improving border surveillance capabilities.

5. **Strengthening Physical Border Infrastructure**

- **Construction of Strategic Infrastructure:** India is focusing on the **construction of strategic infrastructure** such as **border roads**, **tunnels**, and **bridges** to ensure **all-weather connectivity**, enabling quick troop deployment and efficient movement of supplies.
- **Erection of Border Fencing and Floodlighting:** To prevent infiltration and smuggling, the government is installing **border fencing** and **floodlighting** in vulnerable stretches, acting as **physical barriers**.
- **Development of Integrated Check Posts (ICPs):** To streamline trade and travel, **Integrated Check Posts (ICPs)** are being developed along borders. These **modern facilities** bring together **customs**, **immigration**, and **security agencies**, ensuring smoother **cross-border trade** and **regulated movement**.

6. **Managing Border Populations**

Effective border management goes beyond fences and technology; it i**nvolves the people who live in border areas.** These communities are crucial stakeholders, acting as either vulnerabilities or the first line of defense. A successful border strategy must **integrate these communities into the national mainstream and earn their trust.**

- **Denying Local Support to Militants and Insurgents**

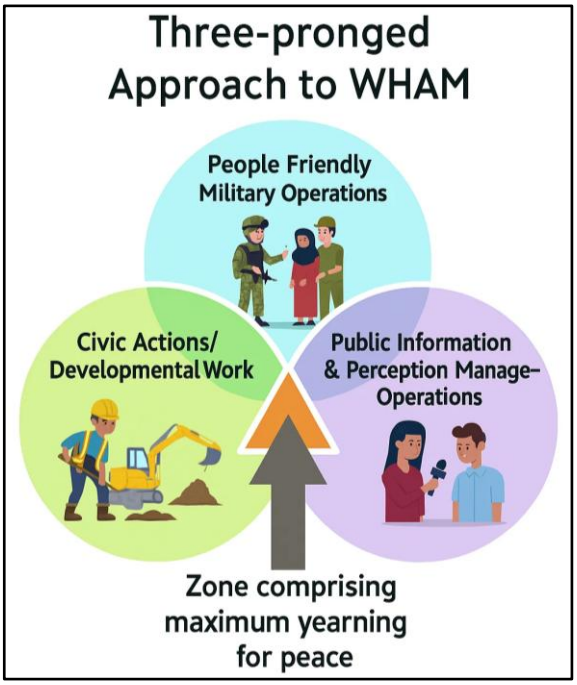
  A core objective of **counter-insurgency** and **counter-terrorism operations** is to **deny local support** to militants and insurgents. These groups are heavily dependent on the local population for:

  - **Intelligence**: Providing information on the movement of security forces.
  - **Logistics**: Offering food, shelter, and medical aid.

Student Notes:

- **Recruitment**: Supplying new cadres.
- **Financial Support**: Through contributions or extortion.

Severing these links isolates militants and weakens their operational capacity, leading to their eventual neutralization.



- **The "Winning Hearts and Minds" (WHAM) Approach**

  To counter hostile propaganda and address the grievances of the border population, security forces have embraced the **"Winning Hearts and Minds" (WHAM)** approach. Key initiatives include:

  - **Operation Sadbhavana**: In Jammu & Kashmir and Ladakh, the Indian Army runs community development projects like schools, medical camps, and vocational training programs for youth, aiming to foster goodwill and support.
  - **Civic Action Programmes**: **Border Guarding Forces (BGFs)** also engage with local populations, offering assistance and building trust through direct interaction.

- **Involving Local Communities in Border Management**

  A proactive strategy involves empowering **local communities** to play an active role in securing the frontiers. This is achieved through:

  - **Village Defence Guards (VDG)**: In Jammu & Kashmir, villagers in remote areas are trained and armed to defend themselves against terrorist attacks, acting as the first line of defense.
  - **Community Policing**: Establishing strong relationships through **community policing** generates valuable human intelligence and fosters shared responsibility for security, ensuring long-term success.

Border defence during Operation Sindoor

For border defence during **Operation Sindoor**, the **Indian Army** used precision-guided **Excalibur artillery rounds** and **loitering munitions** to secure the Line of Control, while the **Border Security Force (BSF)** played a critical role in thwarting infiltration attempts along the International Border. The operation as a whole showcased a new generation of advanced weaponry.

The Spear: India's Offensive Weapons

India's strikes relied on a sophisticated set of precision-guided weapons that allowed for deep penetration and surgical accuracy, all launched from within Indian airspace.

Student Notes:

- **SCALP Cruise Missile:** This is a long-range, stealthy, air-launched missile used for deep strikes against high-value terrorist headquarters far inside Pakistan, such as those in **Muridke** and **Bahawalpur**.
- **BrahMos Cruise Missile:** This is a powerful supersonic air-launched cruise missile. After Pakistan escalated the conflict, India used **BrahMos** missiles to strike key **Pakistan Air Force (PAF) bases**, crippling their operational capacity.

- **HAMMER Munition:** This is an all-weather, precision-guided smart weapon. Fired from **Rafale** jets, **HAMMER** munitions were used to precisely hit terrorist infrastructure in the initial phase of the operation.
- **Loitering Munitions (Kamikaze Drones):** These are "suicide drones" that can circle a target before striking. The Israeli-made **Harop** was used to destroy Pakistani air defence radars, while the **SkyStriker** and the indigenous **Nagastra-1** were used to devastating effect against terror camps.

The Shield: India's Air Defence Systems

One of the biggest successes of the operation was India's robust and **multi-layered air defence architecture**, which effectively neutralized waves of retaliatory Pakistani drone and missile attacks.

- **S-400 Triumf:** Known in Indian service as the **'Sudarshan Chakra'**, this Russian-made long-range system formed the outermost layer of India's defence, capable of engaging threats up to 400 km away.
- **Akash Missile System:** This is an indigenously developed Short-Range Surface-to-Air Missile. Hailed as the "star" of the operation, the **Akash** system had a stellar performance, successfully intercepting multiple incoming drones and missiles launched by Pakistan.

- **Barak-8 MRSAM:** This is a Medium-Range Surface-to-Air Missile system jointly developed by India and Israel. It formed a critical part of the mid-layer of the defensive shield, helping to thwart Pakistani attacks.

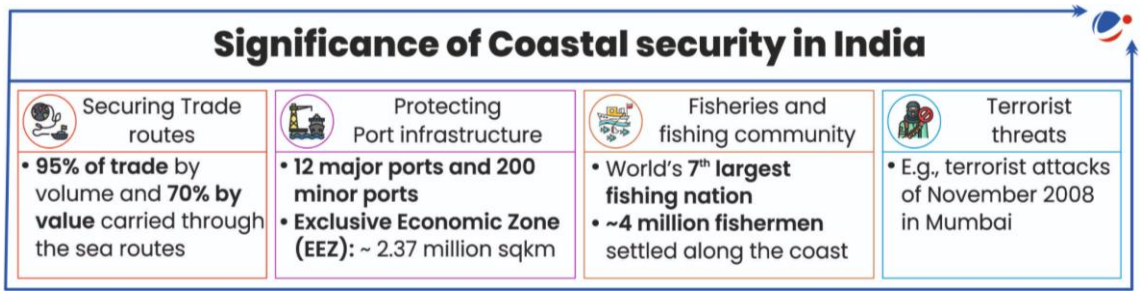
5. Securing the Maritime Frontiers

"In borders, we see the nation's anxieties and aspirations; their management demands the surgeon's precision and the poet's imagination." – Spirit of EU Black Sea Strategy

India's **maritime frontiers**, with a vast coastline of **7,516 km**, pose unique and complex security challenges. The **26/11 Mumbai terror attacks**, in which terrorists infiltrated via the sea route, highlighted vulnerabilities and prompted a complete overhaul of India's coastal security architecture.

India's Coastline

India's coastline recalculated to 11098.81 km from 7561.60 km due to a change in calculation methodology. The **change is due** to a revision in the **methodology**, which now **uses more detailed mapping at a scale of 1:250,000, capturing more intricate features like bays and inlets.**



Unique Challenges:

- **Porous Nature and Vastness**: India's coastline is riddled with **numerous landing point**s, **creeks, small bays,** and **estuarie**s that are difficult to continuously monitor.
- **Proximity to Volatile Regions**: The coasts are adjacent to **politically unstable** and **economically depressed countries**, increasing the risk of **infiltration**, **smuggling**, and **refugee influx**.
- **Piracy and armed robbery:** Piracy by definition **takes place on the high seas** and, therefore, does not fall under the ambit of coastal security. However, in the case of India, the **shallow waters of the Sunderbans have been witnessing 'acts of violence and detention' by gangs of criminals** that are **akin to piracy.**
- **Unsettled Maritime Boundaries**: Disputed maritime boundaries, especially with **Pakistan (Sir Creek)** and **Bangladesh**, create legal ambiguities that criminals and terrorists exploit.
- **High Volume of Maritime Traffic**: The dense traffic of **fishing boats** and **commercial vessels** complicates the identification of suspicious activity.

MARCOS: India's Elite Marine Commandos

MARCOS (Marine Commandos) is the elite special operations force of the **Indian Navy**, established in **1987**, comparable to **US Navy SEALs**.

What Do MARCOS Do?

They specialize in high-risk operations, including:

- **Reconnaissance** and **intelligence gathering**
- **Amphibious warfare**
- **Hostage rescue** and **counter-terrorism**
- **Anti-piracy** and **anti-hijack** missions
- **Underwater sabotage** and **raids**.

They've been involved in missions like the **26/11 Mumbai attacks**.

MARCOS undergo intense training in **combat diving**, **skydiving**, **close-quarter battle**, **counter-insurgency**, and **urban warfare**. MARCOS are key to **India's maritime security**, working with other forces like the **Para (SF)** and **Garud Commando Force**.

Sea Surveillance Excellence

The EU's integrated **Coastal Surveillance Network (CSR)**, a misnomer for the advanced **Common Information Sharing Environment (CISE)**, effectively detects vessels as small as **dinghies**. This sophisticated **maritime technology** enhances security and monitoring across European waters.

This advanced system serves as a valuable **model** for India's comprehensive **three-tier coastal grid**, highlighting the global push for enhanced maritime domain awareness and protection against diverse threats.

5.1. Coastal Security Management

5.1.1. Three-Tiered Security Grid

Post-26/11, India institutionalized a **three-tiered coastal security grid** to provide layered and in-depth security:

Coastal Security Gaps Persist

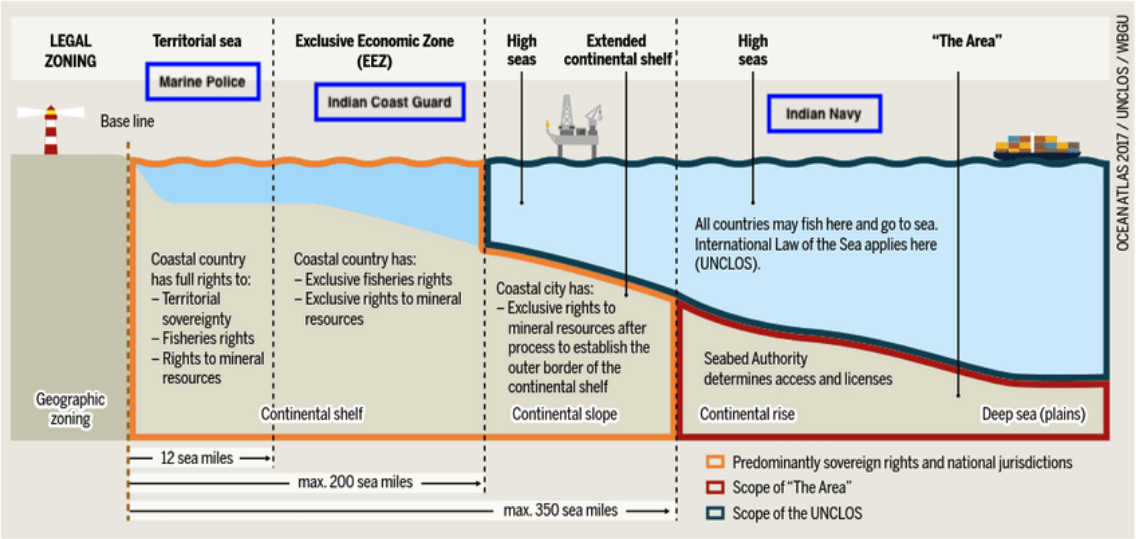
Despite significant **post-26/11 reforms**, **coordination gaps** between the **Navy**, **Coast Guard**, and **Marine Police** persistently hinder India's **coastal security**. This challenge remains evident even in **2024**, impacting overall **maritime vigilance**.

These ongoing **"silos"** in **inter-agency functioning** highlight the critical need for further **integration** and **seamless cooperation** to effectively protect India's vulnerable coastline from diverse threats.

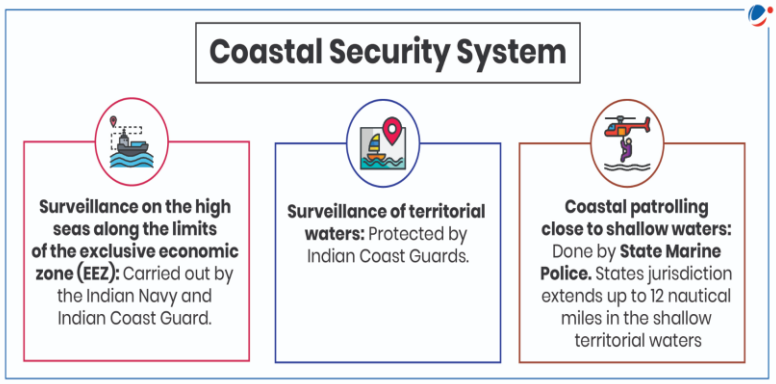
Student Notes:

Student Notes:

- **Indian Navy**: Responsible for **maritime security** on the high seas beyond **200 nautical miles**.
- **Indian Coast Guard (ICG)**: Secures **territorial waters** (up to **12 nautical miles**) and **Exclusive Economic Zone (EEZ)**, crucial in preventing **smuggling**, **poaching**, and **piracy**.
- **State Marine Police**: Patrolling shallow waters (up to **12 nautical miles**) near the coast as part of the **Coastal Security Scheme (CSS)**.



5.1.2. Indian Coast Guard (ICG)



The **Indian Coast Guard (ICG)**, established under the **Coast Guard Act of 1978**, is responsible for **maritime law enforcement**, **search and rescue**, and **marine pollution response**. It operates under the **Ministry of Defence** and plays a vital role in **maritime security**.

The **Indian Coast Guard** enforces **maritime laws**, protects **artificial islands** and **offshore terminals**, ensures **safety of life** and property, coordinates with **customs** for **anti-smuggling** operations, and preserves the **marine environment** while collecting **scientific data**.

Challenges faced by Coast guard	Initiatives taken to strengthen Indian Coast Guard
• **Coordination Issues**: Multiple agencies' involvement causes coordination problems despite efforts like SOPs, joint exercises, and committees. • **Staffing Deficiencies**: Acute staff shortages at police stations, with only 25% of required personnel available. • **Training Gaps**: Absence of a dedicated training academy for	• **Inter-agency Maritime Exercise:** ICG conducts inter-agency exercises like SAREX-2024 and Sagar Kavach to enhance coordination and readiness. • **Increased Responsibility**: In 2009, ICG took on the responsibility for coastal security in territorial waters. • **Coastal Surveillance Network**: A comprehensive network of radars, coastal radar chains, and AIS covers 7,500 km of coastline. • **Joint Operations**: ICG conducts joint operations like KAVACH with Navy and Air Force for improved maritime security.

the Indian Coast Guard limits effectiveness. • **Fishermen's Concerns**: Coastal security depends on fisher communities, but their discontent hinders efficient operations and surveillance.	• **New Patrol Vessels**: ICG commissioned new patrol vessels, including offshore patrol vessels and fast interceptor boats. • **Community Engagement**: Outreach programs promote maritime security awareness among local communities and fishermen.

The **Indian Coast Guard (ICG)** has become a key maritime agency, enhancing **search and rescue frameworks** and supporting **India's SAGAR vision**. Through effective **stakeholder collaboration**, it strengthens India's global reputation as a **reliable maritime partner** in regional security and growth.

5.1.3. Preventing Maritime Piracy in the Indian Ocean

Under Article 101 of the 1982 **United Nations Convention on the Law of the Sea (UNCLOS) piracy** is any act of **violence**, **detention**, or **depredation** carried out on the **high seas** or in areas beyond any state's **jurisdiction** for **private gain**.

Piracy includes actions like **seizing ships**, their **cargo**, or **kidnapping** crew members. Recognized as a serious **maritime crime**, **piracy** is governed by **international laws** and **conventions**, ensuring **global cooperation** for combating these criminal acts.

Consequences of Piracy at Sea/Ocean

- **Threat to Life and Safety**: Piracy puts **seafarers** at risk of injury, **kidnapping**, and **death**, with **hostage situations** being common. Humanitarian and **commercial vessels** are directly endangered.
- **Economic Impact**: Global **economic losses** from piracy range from **$7–25 billion** annually, including **ransom payments**, theft, and delays. Higher **insurance premiums** and security costs for shipping companies increase prices for consumers.
- **Disruption of Trade and Supply Chains**: Piracy disrupts major shipping routes, such as the **Suez Canal**, causing delays and rerouting. This harms **supply chains** and leads to **shortages** and **price hikes**.
- **Increased Regional Instability**: Piracy fuels **political instability** in regions with weak governance, exacerbating **regional insecurity** and undermining **development prospects**.
- **Impact on Humanitarian Aid**: Piracy can delay or halt the delivery of **humanitarian assistance**, risking **food shortages** and **starvation**.
- **Broader Security Threats**: Piracy threatens **navigation safety**, requiring multinational naval action. It also enables **maritime crimes** like **smuggling** and **trafficking**.

Anti-Maritime Piracy Act, 2022

This anti-piracy law targets illegal acts of **violence**, detention, or robbery committed for **private purposes** on the **high seas**, including in India's **Exclusive Economic Zone (EEZ)**. It establishes **Designated Courts** for speedy trials and allows for the **extradition** of accused pirates to other countries.

However, the law faces several legal **concerns**:

Its **death penalty** provision may conflict with **Supreme Court** rulings.

There are ambiguities in what it means to "aid" piracy, which complicates cases and **extradition**.

Despite these issues, the law is crucial. It aligns with India's commitment to the **UN Convention on the Law of the Sea (UNCLOS)** and helps safeguard vital maritime routes like the **Gulf of Aden**, protecting global **maritime trade** from piracy.

National-Level Measures to Combat Piracy

- **Operational Measures**: **Naval ships** with **armed helicopters** actively patrol piracy-prone regions, stationing **Indian Naval** and **Shore Guard ships** along critical coastal zones.

Student Notes:

- **Organizational Measures**: Sharing **ship risk information** boosts **maritime security**; India established the **Indian Ocean International Fusion Centre** in **2018** to improve coordination.
- **Institutional Measures**: The **SAGAR policy** bolsters India's **regional maritime security** responsibilities across the **Indian Ocean** (IOR).
- **Other Measures**: Enhanced **technical surveillance** via systems like **Coastal Surveillance Network** and **National Maritime Domain Awareness** strengthens overall **maritime and coastal security**.

International Measures to Combat Piracy

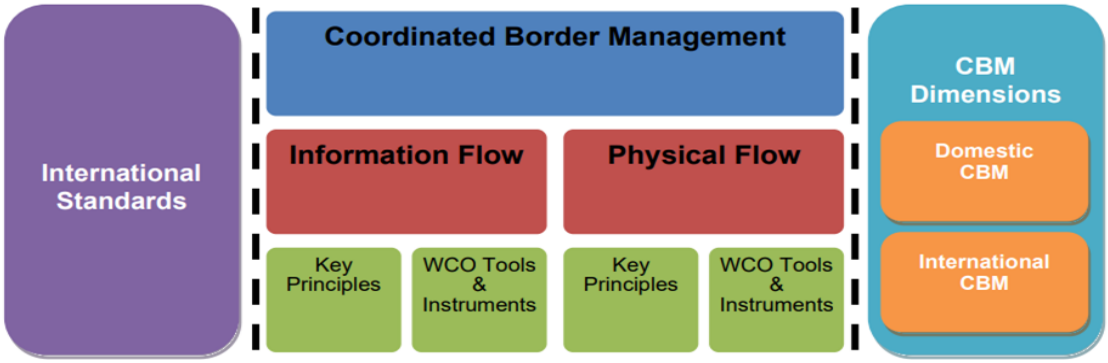
- **UNCLOS**: The **United Nations Convention on the Law of the Sea (UNCLOS)** provides the **legal framework** for **combating piracy** on the high seas and in **exclusive economic zones**.
- **The Convention for the Suppression of Unlawful Acts (SUA) (1988)**: The **Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA)** ensures **appropriate actions** against individuals committing **unlawful acts** like piracy or hijacking of ships.

5.1.4. Post-26/11 Initiatives

In response to the vulnerabilities exposed by the 26/11 attacks, India launched several initiatives to strengthen **coastal security**:

- **Enhancing Maritime Domain Awareness (MDA)**:
  - **National Command Control Communication and Intelligence Network (NC3I)**: A centralized network that integrates data from sensors and databases to monitor maritime activity in real-time.
  - **Information Fusion Centre - Indian Ocean Region (IFC-IOR)**: A hub that shares maritime information regionally and collaborates with international partners to enhance security.
  - **Coastal Surveillance Network (CSN)**: A comprehensive surveillance system with **coastal radars**, **AIS receivers**, and **cameras** for round-the-clock monitoring along the coast.
  - **National Committee for Strengthening Maritime and Coastal Security (NCSMCS)**: Headed by the **Cabinet Secretary**, this body ensures coordination among over 15 central and state agencies involved in coastal security.

These measures ensure a comprehensive, coordinated, and technologically enhanced response to the complex challenges posed by India's maritime security.



Coordinated Border Management (CBM)

Coordinated Border Management (CBM) is a global best practice promoted by entities like the **Inter-American Development Bank (IDB)**. It emphasizes **interoperability** among diverse border agencies.

CBM aims to create a **seamless interface** for border operations, effectively **reducing costs**, enhancing **security**, and significantly **facilitating legitimate trade** across borders through collaborative efforts.

6. Way Ahead: Holistic Approach to Border Management in India

Borders are scars of history, but their management must be a surgery of precision." – Robert Kaplan, The Revenge of Geography

India's **border management** requires coordinated efforts across **security**, **diplomacy**, **administration**, and **development** sectors.

- **Holistic Approach to Border Security**: Adopt a **"Whole-of-Government"** strategy integrating **military**, **diplomatic**, **economic**, and **developmental** efforts to tackle both traditional and non-traditional security threats.
- **Balancing Security with Economic Growth**: Ensure a balance between strengthening **border security** and facilitating **trade** and **people-to-people exchanges**, avoiding negative impacts on **economic growth** in border regions.
- **Enhanced Surveillance and Technology Integration**: Invest in **advanced surveillance technologies** like **CIBMS**, **drones**, and **satellite-based monitoring** to improve border surveillance and address security gaps.
- **Development and Livelihood Creation**: Focus on **socio-economic upliftment** of border populations through initiatives like the **Border Area Development Programme (BADP)** and **Vibrant Villages Programme** to ensure long-term stability.
- **Diplomatic Engagement with Neighbors**: Strengthen **bilateral** and **multilateral dialogue** with neighboring countries to resolve **border disputes**, establish cooperative **border management frameworks**, and enhance **regional security**.

UNIT 6: VARIOUS SECURITY FORCES AND AGENCIES AND THEIR MANDATE

Previous Years Question

- **(2023)** What are the **internal security challenges** being faced by India? Give out the role of Central Intelligence and Investigative Agencies tasked to counter such threats. (250 words/15m)
- **(2019)** The Indian government has recently strengthened the anti-terrorism laws by amending the **Unlawful Activities (Prevention) Act (UAPA), 1967** and the NIA Act. Analyze the changes in the context of the prevailing security environment while discussing the scope and reasons for opposing the UAPA by human rights organizations.
- (2017) Human rights activists constantly highlight the view that the **Armed Forces (Special Powers) Act, 1958 (AFSPA)** is a draconian act leading to cases of human rights abuses by the security forces. What sections of AFSPA are opposed by the activists? Critically evaluate the requirement with reference to the view held by the Apex Court.

1. The Multi-layered Nature of India's Security Apparatus

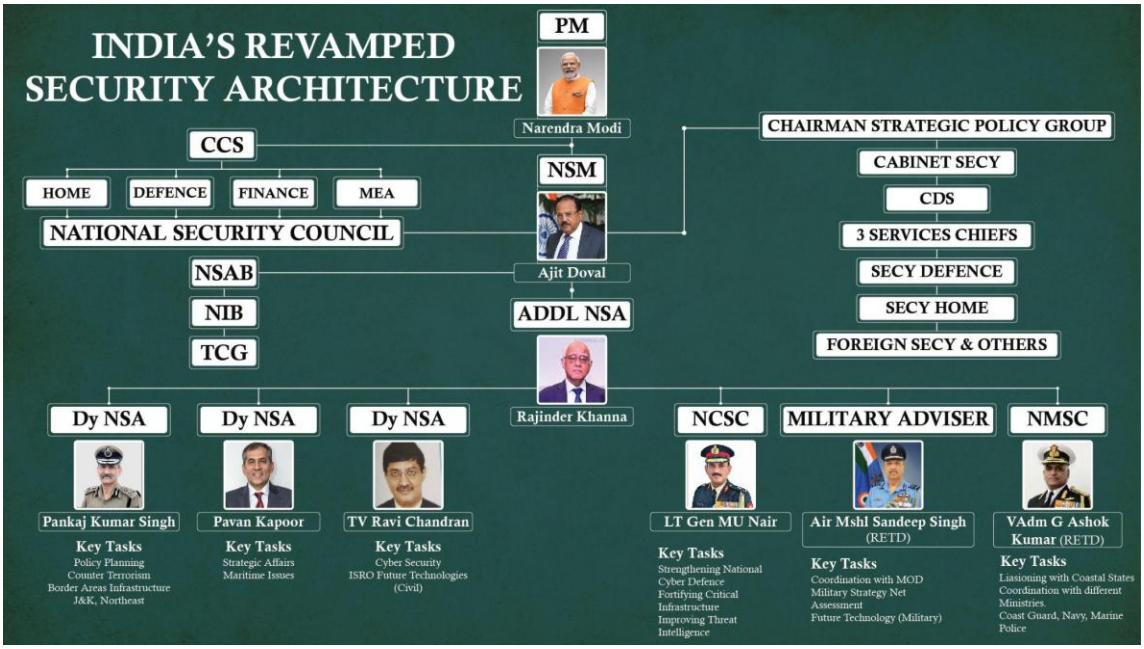
India's internal security apparatus is **multi-layered** and spans multiple levels of governance. The **blurred lines** between state and central powers often lead to challenges in coordination, especially when **multi-state insurgencies** or **cross-border terrorism** are involved.

1.1. Multi-Layered Security Architecture of India

Layer	Union Government	State Governments
Political Layer	Cabinet formulates security policies.	State Governments formulate state-specific policies in cooperation with the Union Govt.
Administrative Layer	Ministry of Home Affairs manages internal security of the nation and coordinates with the various States.	Individual State Govt are responsible for law and order within their territory.
Intelligence Layer	IB, RAW, NTRO collect intelligence.	State Intelligence Units.
Enforcement Layer	CAPFs implement national security policies.	State police and specialized forces enforce state policies on Law and Order.
Constitutional Mandate	Powers defined under Various entries of Seventh Schedule and Articles allowing central assistance to maintain Law and Order in territory of India.	Law and order under State List of Seventh Schedule, States can seek central assistance constitutionally.

Student Notes:

2. National Security Architecture of India



India's national security architecture at its core has the **National Security Council (NSC)**, the **apex body** responsible for advising the Prime Minister on national security and foreign policy matters.The NSC aims to ensure a comprehensive, coordinated approach to India's security.

The **National Security Council Secretariat (NSCS)**, the **executive arm of the NSC**, operates under the **Prime Minister's Office (PMO)** and plays a pivotal role in the implementation of national security policies. It **coordinates the efforts** of various ministries, intelligence agencies, and defense forces to address evolving security concerns. The **NSCS** is **headed** by the **National Security Advisor (NSA)**, who acts as the **principal advisor to the Prime Minister**.

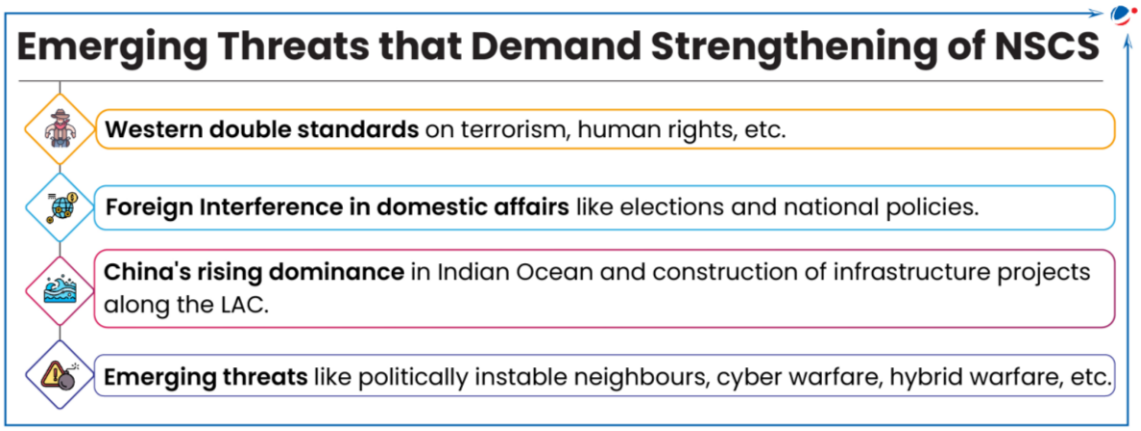
Key Components:

- **Strategic Policy Group (SPG)**: This **inter-ministerial group**, chaired by the NSA, is responsible for coordinating national security policies. It includes **senior officials** from key government bodies like the **Vice Chairman of NITI Aayog**, **Cabinet Secretary**, **Defense and Home Secretaries**, and the **Chiefs of Armed Forces**.
- **National Security Advisory Board (NSAB)**: Comprising retired officials, academics, and experts, the NSAB provides long-term strategic analysis and recommendations on national security issues.
- **National Security Council Secretariat (NSCS)**: The NSCS supports the NSC's objectives and coordinates the activities of various government ministries. It has several verticals, including **Strategic Planning**, **Internal Affairs**, **Intelligence and Technology**, and the **Military vertical**.
- **Joint Intelligence Committee (JIC)**: This body assesses and synthesizes intelligence reports from various agencies such as the **Intelligence Bureau (IB)** and the **Research and Analysis Wing (RAW)**.

Key Tasks of the NSCS:

- **Advising the Prime Minister**: Providing expert advice on strategic assessments, policy options, and crisis management.
- **Formulating National Security Strategy and Policy**: The NSCS helps shape India's long-term security strategy and implements it across various sectors.
- **Coordinating Ministries**: It acts as a central hub for coordinating national security activities across ministries like **Defense**, **External Affairs**, **Home Affairs**, and **Finance**.

- **Monitoring and Assessing Threats**: The NSCS continuously monitors internal and external security threats, including cybersecurity risks, and helps shape India's cybersecurity policies.
- **Overseeing Intelligence**: The NSA heads the NSCS and coordinates intelligence efforts, presenting findings to the Prime Minister.



3. The Central Intelligence, Investigation and Enforcement Agencies

3.1. Intelligence Agencies

Intelligence agencies play a crucial role in **internal security**, gathering information to prevent threats, terrorism, and criminal activities. Key intelligence agencies are **RAW**, **IB**, **NIA**, **CBI** and **National Technical Research Organisation (NTRO)**, ensuring national stability and safety.

3.1.1. Intelligence Bureau (IB)

The **Intelligence Bureau (IB)**, considered the oldest surviving intelligence organization in the world, serves as India's **internal security agency** responsible for mitigating domestic threats.

- The IB falls under the authority of the **Ministry of Home Affairs**.
- The **IB Director** is a part of the **Strategic Policy Group** and the **Joint Intelligence Committee (JIC)** of the **National Security Council (NSC)**.
- The IB Director has the authority to **report directly to the Prime Minister**.

Role of IB:

- **Counterterrorism**: IB tracks individuals, groups, and organizations with suspected terrorist links. It also counters separatist and violent movements, especially in the northeast. The **Multi-Agency Center (MAC)** coordinates intelligence sharing across agencies.
- **Counterintelligence**: IB combats foreign intelligence operations in India using advanced methods like **remote viewing** and **satellite technologies**. Its efforts are vital in preventing espionage.
- **Border Intelligence**: IB collects intelligence along India's porous borders with Pakistan, Nepal, Bangladesh, Bhutan, Burma, and China. It collaborates with border protection forces to monitor and address cross-border threats.
- **Security Threat Assessment**: IB provides threat assessments and security guidelines for VIPs, coordinating with agencies like the **Special Protection Group (SPG)** and state police to ensure safety.

Challenges of the Intelligence Bureau (IB)

- **Coordination Challenges**: Given the large number of intelligence agencies in India, there can be difficulties in ensuring effective coordination and collaboration, which could delay intelligence sharing and strategic decision-making.

Student Notes:

- **Political Surveillance Concerns**: The risk of the IB being used for political purposes, such as surveillance on opposition parties or movements, undermines its credibility and creates trust issues within the public and government institutions.
- **Territorial Reach and Jurisdiction**: The IB's operational scope may face limitations in terms of its **territorial reach**, particularly in remote areas or along international borders, where intelligence collection may be complicated by logistical and security challenges.

Suggestions for Improving IB's Effectiveness

- **Appointment of a National Intelligence Coordinator**: The **Task Force on National Security**, led by former cabinet secretary Naresh Chandra, recommends the creation of a **National Intelligence Coordinator (intelligence czar)** to oversee all intelligence agencies, facilitating effective coordination and enhancing intelligence sharing.
- **Restrict IB to National Security Tasks**: It is advised to **restrict IB's functions** to **national security-related tasks** only, refraining from engaging in **political surveillance**, which would help maintain its impartiality and strengthen public trust.
- **Clarify Territorial Reach of IB and RAW**: Clearly define the **territorial reach** of **IB and RAW** in terms of intelligence collection, ensuring that their activities are well-coordinated, especially in border areas and regions facing external threats.

3.1.2. Research and Analysis Wing (R&AW)

R&AW is India's **external intelligence agency** responsible for intelligence related to **foreign threats, espionage, and counterintelligence**.

Role:

- RAW primarily focuses on **external intelligence gathering** and **countering espionage or covert operations** from foreign powers.
- It has played a significant role in shaping India's foreign policy and national security strategy, contributing to significant successes. Experts point to its role in the creation of Bangladesh in 1971 and enhancing India's nuclear security.
- RAW is said to also control the Special Frontier Force (SFF), a covert paramilitary unit crucial for high-risk operations.

Challenges:

- RAW has faced inter-agency rivalries, particularly with the IB, which can lead to bureaucratic bottlenecks and delays in intelligence sharing and analysis.
- Lack of transparency, with RAW operating largely outside public scrutiny, leading to calls for increased oversight and accountability.

3.1.3. National Technical Research Organisation (NTRO)

NTRO is India's technical intelligence agency, responsible for gathering **intelligence related to cybersecurity, satellite monitoring, and other technical aspects** of national security.

Role:

- NTRO plays a pivotal role in **protecting India's critical infrastructure**, including space technology, communications, and nuclear facilities.
- It is tasked with cyber warfare operations and ensures the technical superiority of India's security infrastructure.

Challenges:

- NTRO has faced criticism for **slow operationalization** and **failure to identify threats** in real-time. For example, it failed to flag key cyber threats, such as the ShyamWitness issue.

Student Notes:

National Intelligence Grid (NATGRID)

Overview & Background:

- **Purpose**: NATGRID is a counter-terrorism intelligence infrastructure designed to connect data from 21 security agencies to help preempt terrorism and locate terror suspects.
- **Operational Since**: December 31, 2020, under the **Ministry of Home Affairs**.
- **Origin**: It was established in response to the **26/11 Mumbai attacks**, which exposed gaps in India's intelligence-gathering and response capabilities.
- **Complementary Agencies**: Part of a larger overhaul of India's security structure, NATGRID works alongside **NIA** and **NCTC** to strengthen intelligence operations and counter-terrorism efforts.

Agencies Connected to NATGRID:

Intelligence Bureau (IB)

Research & Analysis Wing (R&AW)

National Investigation Agency (NIA)

Central Bureau of Investigation (CBI)

Enforcement Directorate (ED)

Directorate of Revenue Intelligence (DRI)

Financial Intelligence Unit (FIU)

Central Board of Direct Taxes (CBDT)

Central Board of Excise and Customs (CBEC)

Directorate General of Central Excise and Intelligence (DGCEI)

Narcotics Control Bureau (NCB)

Functionality:

- **Goal**: To consolidate intelligence from multiple agencies, providing a comprehensive and real-time understanding of potential security threats. The system supports intelligence sharing to identify, track, and prosecute terrorists before attacks occur.
- **Data Sources**:
  - **Immigration Data**: Entry and exit information.
  - **Banking & Financial Transactions**: Tracking financial activities.
  - **Telecom Data**: Monitoring phone records.
  - **Taxpayer Information**: Data on income and tax filings.
  - **Travel Data**: Information on air and train travel.
- **Expansion Plans**: Initially connected to 11 agencies, NATGRID is set to expand to **950 organizations** in the next phases, eventually connecting **1,000 more organizations**.

3.2. Primary Investigative Agencies

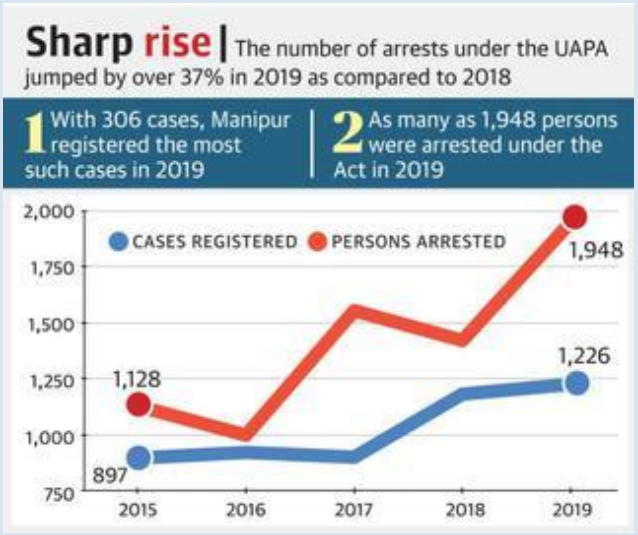
Agency	Establishment	Mandate	Key Challenges	Additional Notes
Central Bureau of Investigation (CBI)	1946 (Renamed in 1963)	Corruption, economic offenses, special crimes, transnational crimes	1. Credibility issues and political interference 2. Operates under weak legal basis (executive order) 3. Inter-state jurisdiction issues requiring state consent	Dubbed as the "caged parrot" by the Supreme Court due to political bias. Lacks strong statutory mandate.
National Investigation Agency (NIA)	Post 26/11	Terrorism-related crimes, human trafficking, cyber-terrorism,	1. Coordination issues with state police	Expanded powers in 2019 to tackle human trafficking,

	Mumbai Attacks	counterfeit currency	2. Lack of resources to handle complex terrorism-related cases	cyber-terrorism, and counterfeit currency.

Student Notes:

Unlawful Activities (Prevention) Act (UAPA)

The **Unlawful Activities (Prevention) Act (UAPA)**, first enacted in **1967**, was introduced to address growing concerns of anti-national activities and secessionist movements. The Act plays a vital role in safeguarding India's **sovereignty**, **integrity**, and **internal security**. Initially created in response to the **Naxalbari uprising**, it has evolved into India's core anti-terrorism legislation over the years, aiming to counter various threats to national security.



History and Evolution:

- **1967**: The UAPA was enacted to deal with activities challenging the integrity of the Indian state, particularly in the context of the Naxalite movement.
- **2004 Amendment**: UAPA was amended to incorporate provisions for combating terrorism after the **Terrorist and Disruptive Activities (Prevention) Act (TADA)** and **Prevention of Terrorism Act (POTA)** were repealed.
- **2008 Amendment**: The law was expanded to allow the **freezing of funds** associated with terrorism and facilitated the establishment of the **National Investigation Agency (NIA)**.
- **2019 Amendment**: UAPA was further updated to include provisions for **cyber-terrorism**, **terrorist financing**, and the ability to designate individuals as terrorists.

Key Provisions:

- **Terrorist Designation**: The central government has the power to declare individuals and organizations as **terrorists**, even without a formal judicial process.
- **Punishment**: Terrorist-related activities can result in **life imprisonment** or **death penalties** depending on the severity of the crime.
- **Investigation by NIA**: The **National Investigation Agency (NIA)** is the principal agency responsible for investigating terrorism-related offenses under the UAPA.
- **Extended Detention and Bail Provisions**: Under the UAPA, suspects

Limitations and Controversies:

- **Broad Definitions**: Critics argue that the definitions of "unlawful activity" and "terrorist acts" are vague and subjective, leading to potential misuse of the law.
- **Low Conviction Rates**: According to the **National Crime Records Bureau (NCRB)**, only **2.2%** of UAPA cases between 2016-2019 led to convictions, raising questions about the law's effectiveness.
- **Bail Restrictions**: UAPA's stringent provisions regarding bail, including denying it unless evidence is proven otherwise, can lead to prolonged detentions, often without conclusive evidence.
- **Lack of Procedural Safeguards**: Critics point out the absence of clear safeguards

can be detained for up to **180 days** without trial, with strict bail conditions, effectively limiting the accused's chances for early release.	against wrongful arrests or designations, especially when governments don't disclose the evidence used to designate individuals or groups as terrorists.

While the **UAPA** serves as an essential tool in the fight against terrorism, its **overreach** and potential **misuse** are significant concerns. The law's broad scope, coupled with **lack of safeguards**, makes it prone to human rights violations. For it to be effective while respecting fundamental rights, there must be a balance between national security and individual freedoms.

3.3. Law Enforcement Agencies

Agency	Role	Challenges
Enforcement Directorate (ED)	Responsible for **enforcing PMLA & FEMA**, focusing on **financial crimes** and money laundering, investigating suspicious financial transactions.	Faces challenges related to the **complexity of financial crimes** and **lack of transparency in operations.**
Financial Intelligence Unit - India (FIU-IND)	Central agency for monitoring financial intelligence related to **anti-money laundering (AML)** and **countering terrorism financing (CFT)**, ensures compliance with global financial standards.	Challenges with **coordination between agencies**, lack of resources to deal with complex financial crimes.
Directorate of Revenue Intelligence (DRI)	**Specialized in smuggling, commercial frauds**, and **illegal trade, monitoring cross-border smuggling activities,** especially drugs, gold, and wildlife trafficking.	Challenges include **resource constraints** and the increasing scale of cross-border smuggling.
Narcotics Control Bureau (NCB)	Works to **combat drug trafficking** and **narco-terrorism**, **prevents narcotics smuggling** that finances terrorism, and coordinates with international agencies like the UN.	Challenges include **increasing drug trafficking** and the need for international coordination to combat narco-terrorism.

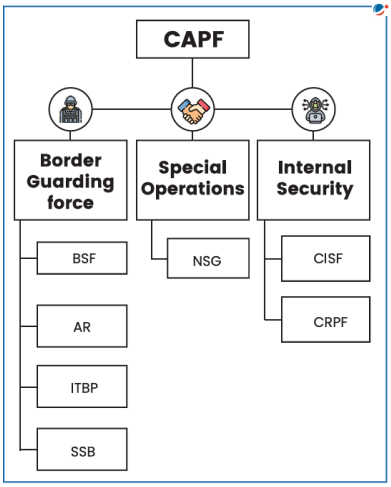
4. Central Armed Police Forces (CAPFs)

The **Central Armed Police Forces (CAPFs)**, also known as **Central Paramilitary Forces (CPMFs)**, are tasked with ensuring India's internal security. They work under the **Ministry of Home Affairs (MHA)** and are crucial for **border protection, counter-terrorism, law enforcement, and assisting in law and order situations**.

Administrative Control

- **Ministry of Home Affairs (MHA)**: The **MHA** is responsible for overseeing the CAPFs, directing their operational activities, and coordinating with other central and state agencies. The MHA also manages the deployment of CAPFs in various internal security issues, including terrorism, insurgencies, and organized crime.
- **Key Responsibilities**:
  - Ensuring **coordination** between central and state agencies.

- **Providing resources**, training, and intelligence sharing.
- Handling **counter-terrorism** and **disaster management** efforts.



Coordination with State Agencies

- **Union-State Collaboration**: The **MHA** facilitates coordination between the central government and states to address internal security challenges.

States often lack the resources to handle certain situations independently, making CAPFs' support indispensable. The **MHA** ensures effective deployment, particularly in areas affected by **insurgency**, **terrorism**, and **ethnic conflict**.

- **Resource Deployment**: CAPFs assist state police in handling complex security concerns by providing specialized forces. Their role spans **border security**, **counter-insurgency operations**, and **crisis management**, ensuring that state and central forces work together in response to evolving threats.

4.1. Border Guarding Forces

The **Border Guarding Forces (BGFs)** are tasked with ensuring the security of India's **international borders**, preventing **illegal immigration**, **cross-border infiltration**, and **smuggling**. Additionally, these forces play a critical role in **counterinsurgency** operations and can be deployed in **wartime** or **peacekeeping missions**.

4.1.1. Border Security Force (BSF)

It was raised in **1965** after the **Indo-Pakistan War** to secure India's borders, particularly those with **Pakistan** and **Bangladesh**. The BSF is currently the **largest border-guarding force** in the world, with **250,000 personnel** spread across **186 battalions**.

- **BSF** holds **powers of arrest, search, and seizure** under multiple legal provisions, including the **Passport Act** and **Customs Act**.
- The motto of the Border Security Force (BSF) is **"Duty Unto Death"**
- **BSF** is the **only CAPF** with its own **Air Wing**, **Marine Wing**, and **artillery units**.
- The force has a **unique Tear Smoke Unit (TSU)**, producing **tear gas munitions** for **anti-riot operations**.

Aspect	Description
Primary Mandate	The **BSF** is tasked with securing **India's borders** with **Pakistan** and **Bangladesh**, covering **6,386 km**. This includes patrolling both **international boundaries** and the **Line of Control (LoC)** in Jammu and Kashmir.
Peacetime Tasks	• Prevents **cross-border infiltration**, **smuggling**, and **illegal entry/exit**. • **Monitors transnational crimes** such as drug trafficking and arms smuggling. • Promotes a **sense of security** among **border populations**. • The Border Security Force has one **Formed Police Unit** deployed with the United Nations Stabilizations **Mission in Democratic Republic of Congo (MONUSCO).**
Wartime Tasks	• Holds positions during conflict, assists the Army in border defense. • **Assists in counterinsurgency** operations, provides **security to critical installations** like airports and nuclear sites.

	• Performing **special tasks** like **intelligence raids** assigned by the Army. • **Anti-infiltration duties** to prevent unauthorized entry at **specified areas**.
Challenges	Due to its multifaceted role, the **BSF** is sometimes diverted from its primary function of **border security** to assist in **internal security operations** like **counterinsurgency** and **riot control**, which may stretch its resources. **Tech Bolsters Border Security** The **BSF** deployed **AI-enabled surveillance drones** along the **India-Pakistan border** in 2024, significantly enhancing security. This **best practice** has notably improved their ability to detect and counter cross-border threats. While specific data varies, these advanced systems have contributed to a substantial **reduction** in illicit activities, including drone-based smuggling, making the border more secure.

4.1.2. Indo-Tibetan Border Police (ITBP)

The **ITBP** was established in **1962** after the **Sino-Indian War** to secure the **India-China border**, particularly challenging high-altitude terrains. Initially designed as a **guerrilla-cum-intelligence force**, it began with and later evolved into a **conventional border guarding force** with specialized capabilities.

- The force's motto is "**Shaurya-Dridhata-Karma Nishtha**" (Valour, Determination, and Devotion).
- Initially part of the **CRPF**, the ITBP became an **independent force** through the **ITBPF Act of 1992**.
- In **2004**, it was recognized as a full-fledged **Central Armed Police Force** under the **Ministry of Home Affairs**.

Key Activities of ITBP

UN Peacekeeping: The **ITBP** has excelled in **UN peacekeeping operations**, serving in **Angola**, **Namibia**, **Bosnia**, **Mozambique**, and **Kosovo**.

Kailash Mansarovar Yatra Security: ITBP has provided **security**, **communication**, and **medical cover** for pilgrims since **1981**.

Disaster Response: ITBP is the **first responder** in the **Himalayas**, establishing **7 Regional Response Centres** for **rescue** and **relief**.

Aspect	Explanation
Primary Mandate	• The **ITBP** secures **3,488 Km** the **India-China** border with altitudes ranging from **9,000 feet to 18,750 feet** in the Western, Middle and Eastern Sector of the **Indo China Border from Karakoram Pass in Ladakh to Jachep La** in Arunachal Pradesh. • Its mandate extends to guarding the **northern border** from **Himachal Pradesh** to **Uttarakhand** and the **Tibet Autonomous Region**.
Duties	• Prevents **illegal immigration**, **smuggling**, and **trans-border crimes**. • Provides **border security** and **surveillance**. • Ensures **security to important installations**, including **hospitals** and **VIPs**.
Special Training	Personnel are trained in **high-altitude warfare**, **survival skills**, and **countering infiltration tactics** used by hostile forces.
Challenges	Although primarily a **border-guarding force**, **ITBP** is occasionally used for **internal security** functions, which can detract from its core mission.

Student Notes:

4.1.3. Sashastra Seema Bal (SSB)

The **SSB** was established in **1963** as the **Special Services Bureau** after the **Chinese aggression** in **1962**.It became a border-guarding force in **2001** after the **Kargil War**.

- In **January 2001**, the **SSB** came under the control of the **Ministry of Home Affairs**.
- In **2001**, the **SSB** was designated as the **Lead Intelligence Agency** for the **Indo-Nepal border**.
- In **2004**, the **SSB** was also tasked with securing the **Indo-Bhutan border**.

Aspect	Explanation
Primary Mandate	The **SSB** guards the **India-Nepal** (1751 km) and **India-Bhutan** (699 km) borders, which are **open borders** with no physical barriers.
Duties	• **Prevents illegal entry**, **smuggling**, and **criminal activities**. • Helps maintain **law and order** in sensitive border regions. • Provides **security to vital installations**.
Additional Roles	• The **SSB** also performs **counter-insurgency** operations in **Jammu and Kashmir** and **anti-Naxal operations** in **Jharkhand**, **Bihar**, and **Chhattisgarh**.

4.1.4. Assam Rifles (AR)

Assam Rifles is **India's oldest paramilitary force**, formed in **1835** as the **Cachar Levy** to protect British tea estates. Renamed in **1917**, it has its headquarters in **Shillong** and is mainly deployed in **Northeastern India** for **counter-insurgency** and **border security** along the **India-Myanmar border**.

- Known as the "**Friends of the North East People,**" it conducts **Civic Action Plans** like building **community halls**, providing **water supply**, and organizing **medical camps**.
- It has played a significant role in **World Wars** and the **Sino-Indian War of 1962**.
- The **dual control structure** makes it unique, with **operational control** under the **Indian Army (Ministry of Defence)** and **administrative control** under the **Ministry of Home Affairs (MHA)**.
- Assam Rifles remains **highly awarded** for its service and has **earned respect** from **local populations** and international bodies, including **UN missions**.

Aspect	Explanation
Primary Mandate	The **Assam Rifles** is tasked with securing **India-Myanmar** borders and conducting **counter-insurgency operations** in India's **North-Eastern region**.
Dual Control Structure	The **Assam Rifles** is unique in that it is run by both the **Ministry of Defence (MOD)** (for operational control) and the **MHA** (for administrative control). This **dual control** has caused issues with coordination and resource management.
Duties	• **Counter-insurgency** operations in **North-East India**. • Provides **rear security** during conflicts and wars. • **Border security** in **India-China** and **India-Myanmar** regions.

Student Notes:

Challenges	**Dual control** results in **coordination problems**, leading to operational inefficiencies. There are also **training issues** as personnel from the **Army** and **MHA** often have conflicting directives.

4.2. Internal Security / Anti-Insurgency Forces

These forces are specialized in **maintaining internal security**, dealing with **terrorism**, **insurgency**, and **internal disturbances**.

4.2.1. Central Reserve Police Force (CRPF)

Formed in **1939** as the **Crown Representative Police** in **Neemuch, Madhya Pradesh**, it was renamed the **Central Reserve Police Force (CRPF)** in **1949** after India's independence. The CRPF's **motto** is "**Seva Aur Nishtha**" (Service and Loyalty).

- The **CRPF** has **6 Mahila (Ladies) Battalions**, making it the only paramilitary force in India with them.

Aspect	Explanation
Primary Mandate	The primary mandate of CRPF is to assist in **maintaining law and order** and **internal security**.
Duties	**Mission and Duties**: • The main objective is to **maintain Rule of Law**, **Public Order**, and **Internal Security**. • Duties include **crowd control**, **riot management**, **counter-militancy**, **counter-insurgency**, and dealing with **Left-Wing Extremism (LWE)**. **Additional Responsibilities**: • Coordinates **large-scale security arrangements** for **elections** in **disturbed areas**. • **Fights enemy forces** in times of war and **participates in UN peacekeeping missions**.
Specialized Units	• **Rapid Action Force (RAF)**: Handles **communal disturbances** and **riots**. • **Commando Battalions for Resolute Action (CoBRA)**:**CoBRA (Commando Battalion for Resolute Action)** is a **specialized force** created to counter **Maoists** and **insurgents** in **Left Wing Extremism (LWE)** affected areas. This unit is also known as **Jungle Warriors**. ○ Raised between **2008-2011**, **10 battalions** have been deployed in **LWE states** like **Chhattisgarh**, **Bihar**, and **Jharkhand**. ○ It is an elite **commando unit**, trained in **jungle warfare** and tactics at the **CoBRA School**, providing exclusive training for survival, combat, and tactics.
Challenges	• Increased **demand for CRPF units** by state governments places stress on resources. • The **CRPF's deployment in multiple duties** causes manpower shortages.

4.2.2. Central Industrial Security Force (CISF)

Founded in **1969**, the **Central Industrial Security Force (CISF)** is one of India's largest CAPFs, originally created to secure **public sector units (PSUs)**. Over time, it expanded its role, **securing vital sectors** related to economic and national security.

With an initial strength of **2,800 personnel**, the CISF now has **188,000 personnel**, securing over **359 establishments** nationwide.

- **Specialized Services**: CISF provides security for **Delhi Metro**, **Parliament House**, and other **critical government buildings**. Additionally, it offers **fire protection services** and safeguards **heritage monuments**.

Aspect	Explanation
Primary Mandate	The CISF secures **strategic sectors**, including **nuclear plants** and **space installations**, **airports**, **ports**, **power plants**, and **heritage sites** like the **Taj Mahal** and **Red Fort**. • **Fire Protection:** It is the **only CAPF** with a **dedicated fire wing**, providing comprehensive **fire protection** to various sectors. It is one of the **largest fire protection service providers** in the country, safeguarding **102 PSUs** with **7,716 personnel** (2018-19). • **Airport Security:** In **2000**, CISF was assigned the task of **airport security** post **IC-814 hijacking**. It now secures **61 domestic and international airports**. • **VIP Protection:** CISF offers **round-the-clock security** to **VIPs** categorized under **Z Plus, Z, X, and Y** security levels. • **Private Sector Security:** Post **Mumbai terror attacks (2008)**, CISF's role expanded to **protect private corporate entities** and offer **consultancy services** for private sector security.
Challenges	The **CISF** faces an increasing workload with more industrial and private-sector **critical installations** requiring security.

Student Notes:

4.3. Specialized Security Forces

4.3.1. National Security Guard (NSG)

Established in **1984**, the **National Security Guard (NSG)** is a specialized counter-terrorism force equipped to handle **high-risk threats** like hijackings, bomb disposal, and hostage rescues. The NSG comprises personnel from the **Army**, **Central Armed Police Forces (CAPFs)**, and **State Police**, focusing on neutralizing terrorist threats.

- **Regional Hubs**: In response to the **26/11 Mumbai attacks**, **four regional hubs** (Mumbai, Chennai, Hyderabad, Kolkata) were set up in **2008**, with a fifth hub established in **Gandhinagar (2016)** to reduce response time across India.
- **Expertise and Reputation**: Known as the "**Black Cats**," NSG commandos are highly trained for **counter-terrorism**, **counter-hijacking**, **bomb disposal**, and **hostage rescue** operations. Their reputation for excellence stems from their high training standards and operational efficiency.
- **Event Security**: NSG units conduct **Immediate Backup Security Operations (IBUS)** for high-profile events like **Republic Day** and **Independence Day**, preventing terrorist attacks.
- **Controversies**: The delayed response during **26/11**, where it took **10 hours** to respond, and operational challenges like **traffic delays** have drawn criticism.
- **Suggestions**: There are calls for **better transportation infrastructure**, **modernization**, and faster expansion of the NSG to improve response efficiency and address existing vulnerabilities.

The **2008 Mumbai attacks** were a critical **turning point**, highlighting delays in counter-terror response. In direct consequence, the **NSG** (National Security Guard) established **4 regional hubs** across India.

These hubs, including Mumbai, Kolkata, Hyderabad, and Chennai, ensure **rapid response** by elite commandos, significantly reducing deployment times during future terror incidents.

Aspect	Explanation
Primary Mandate	The **NSG** is tasked with handling cases like **terrorist attacks**, **counter-hijacking operations**, and **bomb disposal**.
Duties	• **Counter-terrorism** operations and **VIP protection**. • **Sky marshals** for **aviation security**. • Provides **security to critical installations**. • NSG's specific tasks include handling **hijacking situations**, **bomb disposal**, **post-blast investigation**, and providing **close protection**.
Challenges	• The **NSG** faces **operational inefficiencies** due to **staff shortages**, **bureaucratic inefficiencies**, and **lack of modern equipment**.

Elite Force, Global Training

India's **NSG "Black Cat" commandos** consistently train with world-renowned counter-terrorism units like **Germany's GSG 9** and **Israel's Yamam**. This collaboration ensures the adoption of **best practices**, including tactics like **"flash-bang" grenades**, enhancing India's elite force capabilities.

Student Notes:

5. Role of Armed Forces in Internal Security

In India, responsibility for **internal security** primarily falls under the **Ministry of Home Affairs (MHA)**. The **Indian Armed Forces**—comprising the **Army, Navy, and Air Force**—play an essential but secondary role, providing support to the civilian administration only when threats escalate beyond the capacity of police and paramilitary forces.

When deployed for such tasks, the armed forces report to the **Ministry of Defence** and act under the constitutional authority of the **President of India**. To handle these complex internal threats, they have developed highly **specialized units**, including the Army's **Rashtriya Rifles**, the Navy's **MARCOS**, and the Air Force's **Garud Commando Force**.

Counter-Insurgency Operations:

- The **Indian Army** plays a key role in counterinsurgency operations, especially in **Jammu and Kashmir** and the **North Eastern states**.
- **Rashtriya Rifles (RR):** A specialized military unit formed in the 1990s, **RR** focuses on **counterinsurgency** in Jammu and Kashmir.

Rashtriya Rifles: India's Elite Counter-Insurgency Force

Rashtriya Rifles (RR) is a specialist **counter-insurgency** force under the **Indian Army**, formed in **1990** to combat insurgency and terrorism, mainly in **Jammu & Kashmir**. It is composed of personnel drawn from various Army regiments, making it an all-**Army composite unit**.

Role & Functions:

- Conducts **anti-terrorism** and **counter-insurgency operations**.
- **Area domination**, **intelligence gathering**, and **target neutralization**.
- Assists **civil authorities** in restoring peace and order.
- Runs **civic action programs** to build trust with local communities.

Position in Defence System: RR is India's largest and most experienced **counter-insurgency force**, directly controlled by the Indian Army, known for its effectiveness in high-conflict zones.

Motto: **"Dridhta aur Veerta"** (Determination and Valour).

Aid to Civil Authorities:

- The Armed Forces assist during communal riots, large-scale violence thereby helping in restoring law and order when requested by the government

Disaster Response:

- The Indian Armed Forces are frequently deployed during natural disasters, such as earthquakes, floods, and pandemics.
- Their roles include:
  - **Search-and-rescue operations**
  - **Providing medical and food assistance**
  - **Restoring infrastructure** (roads, bridges)
  - **Ensuring security** in disaster-affected areas

Armed Forces Special Powers Act (AFSPA):

- Enacted in 1958, AFSPA grants military forces extraordinary powers in regions with insurgent activity, primarily in Jammu & Kashmir and the North East.
- The Act allows the military to **use force**, conduct **searches without warrants**, and **detain suspects without trial** in "disturbed areas".
- **Criticism:** AFSPA has faced significant opposition for **human rights violations**, including allegations of **fake encounters** and **torture**.

AFSPA: A Contentious Divide

The **partial AFSPA revocation** in **Nagaland** (2022/2023), sparked by the tragic **Oting killings**, ignited intense debates. It starkly highlights the conflict between **human rights** and perceived **operational necessity** for security forces.

This contentious issue, a recurring theme in India's Northeast, has even been a direct question in the **UPSC** examinations, underscoring its national significance.

Student Notes:

5.1. Key Joint Military Exercises of India

India regularly conducts joint military exercises with various countries to enhance **interoperability**, **readiness**, and **defence cooperation**. These exercises focus on different domains such as **army**, **naval**, and **tri-service** operations. The exercises strengthen partnerships and help in sharing best practices, counter-terrorism strategies, and disaster response tactics.

Exercise	Participating Countries	Domain	Brief Description
Yudh Abhyas	India, USA	Army	Annual exercise focusing on **high-altitude warfare**, **joint operations**, and sharing best practices.
Malabar	India, USA, Japan, Australia	Naval	Multinational exercise enhancing **maritime security** and **interoperability** among **Quad** nations.
Varuna	India, France	Naval	Bilateral exercise fostering **maritime cooperation** and **naval operational skills**.
Shakti	India, France	Army	Biennial exercise focusing on **counter-terrorism** and **joint military operations**.
Nomadic Elephant	India, Mongolia	Army	Annual **counter-insurgency** and **jungle warfare** training exercise.
Surya Kiran	India, Nepal	Army	Annual exercise promoting **bilateral army cooperation** and **operational readiness**.
Sampriti	India, Bangladesh	Army	Annual exercise focusing on **counter-terrorism** and **border security cooperation**.
Hand-in-Hand	India, China	Army	Recurring **confidence-building** measure for **counter-terrorism** and **disaster response**.
Tiger Triumph	India, USA	Tri-service	Joint **Navy**, **Army**, **Air Force** exercise for **humanitarian assistance** and **disaster relief**.
Vajra Prahar	India, USA	Army Special Forces	Annual special forces training focused on **counter-terrorism** and **interoperability**.

6. State Police Forces and Their Mandate

In India, the **police system** is primarily structured under **state jurisdiction**, with support from the Union Government in certain situations.

- **State Responsibility**: **Police and public order** are under the **State List** (List II) of the **Seventh Schedule** of the Constitution.
- **Support of Union**:
  - **Article 355**: The **Union Government** is **obligated to protect states** from internal disturbances and ensure the government operates according to the Constitution.
  - **State Intervention**: The **Union Government** can intervene if a state is unable to maintain law and order or control internal disturbances.

Student Notes:

- **Union Support**: The **Union Government** thus provides **intelligence**, **financial aid**, and **Central Armed Police Forces (CAPFs)** when states require assistance or there is an emergent situation.

6.1. Structure and Hierarchy

The Indian police system is structured to manage law and order across the country, with significant roles assigned to state police forces. The **Police Act of 1861** governs the structure, which has evolved to include various specialized units addressing specific challenges.

Police Organization:

- The **State Police** is structured across multiple hierarchical levels.
- **District-level units** handle day-to-day law enforcement, under the supervision of district police heads.
- **Specialized Crime Branches** focus on specific criminal activities, such as organized crime, drug trafficking, and corruption.
- **Regional Divisions** coordinate between various districts and help in managing law and order over larger territories.
- **Police Headquarters** in each state manage overall operations and resource allocation.

Specialized Units:

- **Anti-Terrorism Squads (ATS):** These units handle terrorism-related issues and organized crime.
- **Special Task Forces (STF):** Created for specific threats like insurgency or high-profile criminal activities.
- **Cyber Police:** Established in some states to deal with growing cybercrimes.
- **Economic Offenses Wing (EOW):** These wings focus on tackling financial crimes, fraud, and corruption.

Battling Digital Jihad

The **Maharashtra ATS** recently busted an **ISIS-inspired module** in **Pune**, with investigations continuing into **2025**. This crucial operation heavily relied on **cyber-forensics**.

The case highlights the escalating threat of **digital radicalization**, where terror groups leverage online platforms for recruitment, indoctrination, and operational planning.

As noted earlier, while l**aw enforcement is primarily the responsibility of the state**, the U**nion Government supports through intelligence sharing, coordination with CAPFs**, and resources for national security.

Bridging the Forensic Gap

India faces a significant **forensic modernization gap**, with a low percentage of police stations having **digital forensics labs**. In contrast, the **UK** boasts more integrated capabilities, highlighting disparities in infrastructure.

However, **Delhi Police's CyPAD unit** is a **replicable model**, successfully clearing numerous **cyber cases** in 2024. Its use of advanced forensics showcases a path to bridge this critical investigative gap.

6.2. Challenges Faced by State Police

- **Modernization Deficit**: There has been **inadequate funding** for **modernizing** police forces, affecting areas like **technology**, **training**, and **infrastructure**. The **police force** continues to use outdated equipment and lacks sufficient technological advancements for modern policing needs.
- **Overburdened Police Force**:
  - **Increased Crime**: Crime rates have increased by **28%** over the past decade, while **police personnel** per lakh population stands at **137**, far lower than the **UN's recommended 181** and **222**.
  - **Understaffed Forces**: The inadequate number of police officers makes it harder to **manage crimes** and respond effectively to **emerging security threats** like **terrorism** and **cybercrime**.

Student Notes:

- **Quality of Investigations**:
  - **Low Conviction Rate**: The **conviction rate** for crimes stands at just **47%**, largely due to **lack of training** in criminal investigations and insufficient **legal knowledge** and **forensic resources**.
  - **Outdated Infrastructure**: There is a **lack of forensic labs**, **cybercrime units**, and **trained officers**, leading to poor-quality investigations and a **lower conviction rate**.

Police Modernization: A Tech-Driven Future

India's **police forces** are undergoing continuous **modernization**, a long-standing "Best Practice." The **Ministry of Home Affairs** allocates substantial annual funds, with **₹4,069.24 crore** budgeted for Police Modernization in **2025-26**.

This investment prioritizes **AI-enabled CCTV** for enhanced surveillance and the **National Automated Fingerprint Identification System (NAFIS)**. These technologies are crucial for improving crime prevention, investigation, and overall law enforcement capabilities.

- **Police Accountability**: **Political interference** in police matters often leads to **abuse of power**, **criminalization**, and **corruption** within the force. **Police decision-making** becomes compromised due to political pressure, affecting **independence** and **objectivity**.
- **Lack of Infrastructure**:
  - **Outdated Equipment**: Police forces face delays in **procuring new equipment**, **vehicles**, and modern **technology**. Many **police stations** are under-equipped, and training academies often suffer from **poor infrastructure**.
  - **Training Deficiencies**: **Police training** often fails to address modern challenges, including **cybercrime** and **advanced forensic procedures**.

Janamaithri Suraksha Project-People-Friendly Policing

Kerala's **"Janamaithri Suraksha Project"** is an authentic, acclaimed **community beat policing** initiative. Launched in 2008, it fosters police-public trust through dedicated **beat officers**, effectively enhancing **crime prevention** via citizen participation.

- **Public Perception**:
  - **Negative Image**: The public perceives the police more as **trouble creators** than **trouble-shooters**, with high levels of **corruption** and **abuse of power** being common complaints.
  - **Community Cooperation**: The police heavily depend on **community cooperation** for **crime investigations** but often fail to build trust due to poor relations with the public.
- **Human Rights Concerns:** Significant **human rights violations**, such as **custodial deaths, encounter killings,** and **police brutality**, persist. These issues reflect systemic problems within the police forces, including a lack of accountability, poor working conditions, and insufficient training in human rights.

Modernization of Police & Police Reforms

MPF Scheme (Modernization of Police Forces)

The **MPF Scheme** was initiated in **1969-70** to modernize police forces across India. In recent years, the fund allocation has been **increased**, reflecting a **commitment** to improve **policing infrastructure** and **law enforcement capabilities**. **Key Features**:

- **Improving Law and Order**: Focus on enhancing police capacity for maintaining **internal security**, especially in areas vulnerable to **left-wing extremism**, **terrorism**, and **organized crime**.
- **Women's Security**: The scheme allocates funds for enhancing **women's security** by providing **specialized units** for addressing crimes against women.
- **Infrastructure Development**: Funds are allocated for upgrading **police stations**, acquiring **modern weapons**, improving **police mobility**, and setting up **forensic science labs**.

- **Training & Equipment**: The scheme promotes the **modernization of police training academies**, equipping police with **advanced technology** for **cybercrime investigations**, **surveillance**, and **crime tracking**.
- **Linking Criminal Justice System**: Integration with the **Crime and Criminal Tracking Network and System (CCTNS)** and other critical pillars like **prisons**, **prosecution offices**, and **forensic labs.**

Prakash Singh Case (2006) – Supreme Court Judgment

The **Prakash Singh case** (2006) involved the Supreme Court's landmark ruling, which recommended a series of **police reforms** to improve the **independence**, **accountability**, and **professionalism** of the Indian police. The Court issued **comprehensive directions**:

- **State Security Commissions (SSCs)**: Create **autonomous bodies** to ensure **independence** of police forces from political influence.
- **Police Establishment Boards (PEBs)**: Establish **boards** to handle **transfers**, **promotions**, and **appointments** within the police, reducing **political interference**.
- **Police Complaints Authority (PCA)**: Set up independent authorities at the **state and district levels** to investigate police misconduct and ensure **accountability**.
- **Director General of Police (DGP)**: Ensure the **DGP** is selected from the **top three senior-most officers**, with a **two-year tenure** to provide **stability** and **continuity** in leadership.
- **Separation of Investigation and Law Enforcement**: Create separate wings for **investigation** and **law enforcement** to improve the **quality** and **effectiveness** of criminal investigations.

Justice Thomas Committee: The **Justice Thomas Committee** was tasked with monitoring the implementation of the Supreme Court's directives in the **Prakash Singh case**.

- It reported that some states did not fully comply with the Court's suggestions, especially regarding the composition of the **State Security Commissions** and the **Police Establishment Boards**.
- The committee emphasized **tenure security** for officers and recommended that **DGPs** be selected from the **senior-most officers**, ensuring a minimum two-year tenure.
- The Committee also stressed the need for proper infrastructure, training, and independent operations for **investigating police**.

Despite the SC's directions, many states have **failed to implement** the recommendations. There are issues with the **composition** and **powers** of **SSCs**, and many states continue to have **political control** over police forces. The **removal of officers** on arbitrary grounds, as seen in cases like **T.P. Senkumar** (Kerala), reflects the **lack of security of tenure.**

6.3. Recommendations for Reform

- **Increase Police Personnel**: To meet the increasing crime rates, the **number of police personnel** should be raised in line with **UN recommendations** (181 per lakh population).
- **Infrastructure & Technological Upgrades**: Invest in modernizing **police infrastructure**, improving **training**, and providing **advanced equipment** like **cybercrime units** and **forensic labs**.
- **Separation of Investigation and Law Enforcement**: Establish **separate wings** for **investigation** and **law enforcement** to improve the **quality of investigations** and reduce overburdening of police officers.
- **Leadership Reform**: Ensure **fixed tenure** for key leadership positions like **DGP** to maintain **continuity** and **stability** in police operations.
- **Enhanced Accountability**: Set up independent **Police Complaints Authorities** at **state and district levels** to address **police misconduct** and ensure **transparency**.

Student Notes:

7. Challenges and Reforms in India's Security Apparatus

Challenges	Details
Inter-Agency Coordination Gaps	
Intelligence Sharing Challenges	**CBI** and **IB were criticized** for poor coordination and delayed responses, e.g., 26/11 Mumbai attacks.
	MAC and **NATGRID** efforts hampered by turf wars and political resistance.
	State police find **IB's intelligence vague**, complicating actions during crises.
MHA-MoD Turf Wars	**Assam Rifles** faces **dual control** under **MHA** and **MoD**, leading to **complex management**.
	CAPFs face **mission creep**, causing **resource misallocation**.
Centre-State Coordination Issues	**State governments** often rely on the **Centre** for resources and coordination, especially in high-risk areas.
	Conflicts between **federal** (e.g., **CBI**) and **state governments** erode state power, creating a fragile balance in internal security.
Modernization & Capacity Building	
Technological Upgrades	**Cybercrime** is on the rise, with **attacks on Aadhaar** and critical systems.
	CCTNS faces **implementation delays** due to data quality issues and outdated technology.
	NATGRID was delayed due to internal conflicts over intelligence sharing.
Training and Skill Development	**The training budget** was just **1.13%** in 2019-2020, and specialized **cybercrime training** is lacking.
	State police are often **underprepared** for evolving challenges.
Infrastructure Gaps	**Police stations** lack essential equipment, and many **state forces** are **underequipped** with modern weaponry.
	Forensic labs suffer from **poor infrastructure**, leading to delays and weak criminal justice.
Human Resource Challenges	
Understaffing & Recruitment	**Police-to-population ratio** in India is low (**1.58 officers per 1000 people**).
	High **vacancy rate** (25%) and **manipulation** in recruitment processes, especially for constables.
	Police personnel face **long hours** with insufficient leave or training.

Student Notes:

Welfare & Working Conditions	**Outdated Police Act 1861** assumes civil police should operate like soldiers, leading to **overwork** and poor conditions.
Attrition & Motivation	High **suicides** and stress levels indicate **poor morale** and alienation.
	Overburdened and **underprepared forces** lead to **poor motivation** and **high attrition** rates.
Accountability & Human Rights Concerns	
Excesses and Lack of Oversight	**AFSPA** grants immunity to security forces, despite **human rights violations** like extrajudicial killings and torture.
	CBI, **NIA**, and **IB** operate with minimal **oversight** and face **credibility issues** due to political influence.
Balancing Security with Human Rights	**Preventive detention laws** and **extraordinary powers** under **AFSPA** and **counterterrorism laws** often infringe on civil liberties.
	The **Supreme Court** has prioritized **public order** over individual rights, making it cautious in dealing with human rights violations.

7.1. India's Integrated Theatre Commands (ITC)

India's transition to **Integrated Theatre Commands (ITCs)**, set for 2025, is a major **military reform** aimed at improving **coordination** and **operational synergy** among the **Army**, **Navy**, and **Air Force**. By consolidating control under unified commands for specific regions, the ITCs seek to enhance **efficiency**, **speed**, and **coordination** during both **wartime** and **peacetime operations**.

Theaterisation Plan

India's **"Theaterisation"** plan integrates the **Army**, **Navy**, and **Air Force** under single **theatre commanders** responsible for geographical or functional areas. This model is inspired by the **US Unified Command Plan**, which consists of 11 combatant commands.

Operational Control

The **Chief of Defence Staff (CDS)** oversees operational control of the ITCs. The **service chiefs** remain responsible for **training**, **equipping**, and **administering** their respective forces. **General Bipin Rawat** was India's first CDS (2019–2021), followed by **General Anil Chauhan** (2025).

Current Structure

Before the ITC reform, India had:

- **17 single-service commands**: 7 Army, 7 Air Force, 3 Navy.
- **2 tri-service commands**:
  - **Andaman and Nicobar Command (ANC)**: India's only fully operational tri-service command.
  - **Strategic Forces Command (SFC)**: Handles India's nuclear arsenal.

Key Developments in 2025

- **New Legislative Framework**: The **Inter-Services Organisations (Command, Control, and Discipline) Act, 2023** gives theatre commanders full control over personnel from all services, strengthening joint operations.
- **Headquarters Designations**:
  - **Northern Theatre Command (Lucknow)**: Focuses on the **China border**.
  - **Western Theatre Command (Jaipur)**: Focuses on the **Pakistan border**.
  - **Maritime Theatre Command**: Likely in **Karwar** or **Mumbai** (discussions continue).
- **Operational Timeline**: ITCs are expected to be **phased in** by 2026, with full operational status by **2027/2028**.

- **Cyber, Space, and Special Operations**: The ITC reform includes integrating **cyber**, **space**, and **special operations** units to address modern **warfare** and **technology-driven threats**.

Strategic Objectives of ITCs	Challenges in Implementing ITCs
• **Improved Coordination**: ITCs ensure better collaboration and interoperability between the Army, Navy, and Air Force, facilitating joint operations. • **Resource Optimization**: Streamlined operations reduce redundancy and improve logistics management. • **Faster Decision-Making**: Unified command allows quicker responses to security challenges. • **Modern Warfare Readiness**: ITCs integrate new capabilities in cyber, space, and information warfare.	• **Cultural Integration**: The merging of diverse operational cultures from each armed service presents a challenge. • **Inter-Service Rivalry**: Balancing priorities and interests between the services may lead to friction. • **Implementation Complexity**: The structural overhaul required for ITCs demands careful planning and execution.

7.2. The Changing Face of Combat: Women in Action

Women in the **military** have gradually shifted from **auxiliary** and **support roles** to **active combat positions**. They now serve in **frontline combat units** such as **infantry**, **special forces**, and **aviation**. Many nations have begun integrating women into roles traditionally reserved for men, highlighting their capabilities in **modern warfare**.

- In **2021**, the **Supreme Court** allowed **women's admission** to the **National Defence Academy (NDA)**. The **first female batch** joined in **2022**. Established in **1954** at **Khadakwasla**, NDA is the world's **first tri-service academy**, training cadets from the **Army, Navy, and Air Force**.
- The **Supreme Court** has **directed the Centre** to ensure that women are granted **permanent commission (PC) in the Indian Coast Guard (ICG),** stating that if the government doesn't, the court will intervene.

Leading from the Front: Women's Impact in Operation Sindoor

Operation **Sindoor** saw two prominent **women officers**, **Colonel Sophia Qureshi** and **Wing Commander Vyomika Singh**, play key roles. They led the **media briefing** on India's **military response** to **terrorist camps** in **Pakistan**, reflecting India's **inclusive defense strategy** and women's growing **leadership** in the **armed forces**.

Colonel **Qureshi**, an officer in the Army's **Corps of Signals** with **UN peacekeeping experience**, and **Wing Commander Singh**, an expert **helicopter pilot**, represented the **operational excellence** of **women** in India's **defense**. Their **leadership** marked a significant milestone in **gender inclusivity** within the armed forces.

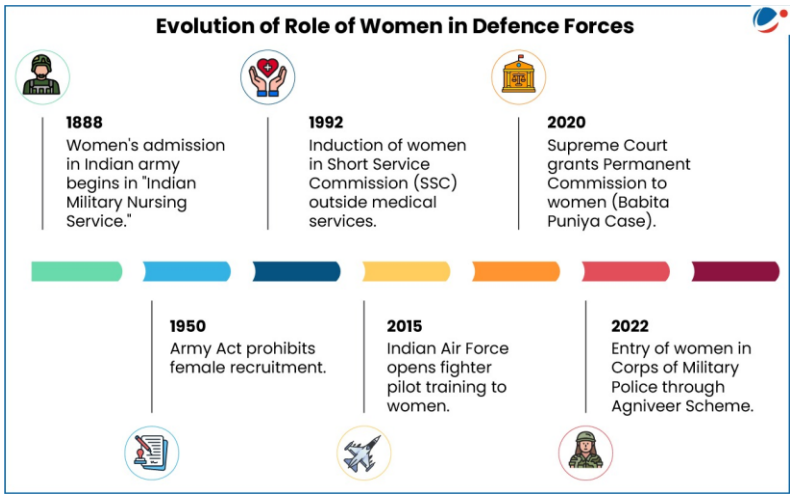
Significance of Women Participation in Defense Forces	Challenges Faced by Women in Combat
• **Gender Equality**: Women's participation in the defense forces aligns with **constitutional principles** of **equality** (Articles 14, 15, 16), promoting **non-discriminatory** opportunities and fostering a culture of **equal rights** and **access** to all positions within the military. • **Talent Pool and Recruitment**: In the era of **cyber warfare** and **digitally equipped weapons**, women can play a crucial role, as they possess	• **Physical and Mental Demands**: **Combat roles** require intense **physical** and **mental stamina**, and women often face higher scrutiny due to preconceived notions about their **physical capabilities**. • **Gender Bias**: Despite progress, women in combat still face **gender biases**, including **discrimination**

Student Notes:

the skills to handle advanced **technology** and **weaponry**, contributing to a **diverse** and **capable** workforce. • **Humanitarian Role of Defense Forces**: Women can effectively engage with **local populations** in **conflict zones**, particularly in regions where societal norms may limit the interactions of **male soldiers**, enabling the military to carry out **Military Civic Action programs** successfully. • **Humanitarian and Peacekeeping Missions**: Women's **presence** in **peacekeeping missions** allows for building **trust** and fostering connections with **local populations**, especially in **culturally sensitive** areas where women may feel more comfortable interacting with female soldiers rather than male counterparts.	from their male counterparts, which can hinder their **performance** and **integration** into combat units. • **Sexual Harassment**: A pervasive issue across many militaries is the prevalence of **sexual harassment**. Women in combat often encounter inappropriate behavior, creating a **hostile work environment** that can disrupt operations. • **Workplace Inequality**: Women in combat roles sometimes experience **unequal opportunities** for advancement, **training**, and **leadership positions** due to systemic **biases**.

Suggestions for Improvement

- **Policy Revisions**: Governments should create **policies** that fully support **gender equality** in **combat roles**, ensuring **equal access** to all positions, training, and promotions for women in the **military**.
- **Combat-Specific Training for Women**: Tailored **fitness** and **combat training programs** should be developed to address the unique **physical needs** of female soldiers, ensuring they are fully prepared for the demands of their roles.



- **Zero Tolerance for Harassment**: Strict **policies** should be implemented to prevent and address **sexual harassment** and **gender-based violence** within **military forces**, ensuring a safe and supportive environment for all soldiers.
- **Leadership and Mentorship Programs**: Establish **mentorship** and **leadership development programs** for women to ensure they are equipped to take on higher ranks and leadership roles, promoting **career advancement**.
- **Public Awareness and Cultural Change**: **Public awareness campaigns** should challenge traditional **gender stereotypes** and highlight the contributions of women in **combat**, fostering broader **acceptance** within **society** and the **military**.

By implementing these measures, the military can build a more **inclusive**, **effective**, and **diverse** force, where both men and women serve equally in defense of their countries.

VISIONIAS
INSPIRING INNOVATION

OUR ACHIEVEMENTS