CHANAKYA
IAS ACADEMY
Nurturing Leaders of Tomorrow
SINCE 1993

CIVILS WITH AKASH

MAINS BRAINBOX

PCS NOTES FOR

INTERNAL SECURITY

COMPILED BY: AKASH SIR, IAS AADITYA SHARMA,
ABHINANDAN GUPTA

OUR DIGNITARIES

ISHAN SINGLA
(DSP, PCS 2020)

MOHIT SINGLA
(DSP, PCS 2018)

Mr. Harmanpreet Cheema
DSP Ghanaur (Patiala)

Mr. Chander Shekhar, IAS Retd.
Member,
Haryana Real Estate Regulatory Authority, Panchkula

Ms.Shashi Prabha Dwivedi
(DGP) Punjab Police

ਬੇਦਾਅਵਾ,,,,
ਅਸੀ ਹੱਕ ਮੁਜ਼ਬ ਨਾਲ ਤਸਲੀਮ ਕਰਦੇ ਹਾ,
ਇਹ ਨੋਟਸ ਬਹੁਤ ਮਿਹਨਤ ਦੇ ਨਾਲ, ਅਕਾਸ਼ ਸਰ,
ਅਭਿਨੰਦਨ ਗੁਪਤਾ, ਅਤੇ ਆਈ. ਏ. ਐਸ. ਆਦਿੱਤਯ ਸ਼ਰਮਾ
ਵਲੋਂ ਮਿਲ ਕੇ ਤਿਆਰ ਕੀਤੇ ਗਏ
ਹਨ। ਇਨ੍ਹਾਂ ਦੀ ਤੁਲਨਾਂ ਬਾਕੀ ਮੁਫ਼ਤ ਵਾਲੇ ਨੋਟਸ
ਨਾਲ ਨਾ ਕੀਤੀ ਜਾਵੇ ਅਤੇ ਨਾ ਹੀ ਨਕਲ ਕੀਤੀ
ਜਾਵੇ,ਕਰਤਾ ਦੇ ਸਭ ਹੱਕ ਰਾਖਵੇਂ ਹਨ।ਧੰਨਵਾਦ ਜੀ।

CHANAKYA
IAS ACADEMY
Nurturing Leaders of Tomorrow
SINCE 1993

CIVILS WITH AKASH

INTERNAL SECURITY

Issues related to Security

3.1 Linkages between development and spread of extremism;

3.2 Role of external, State and non-State actors in creating challenges to internal security; Challenges to internal security through communication networks; role of media and social networking sites in internal security challenges,

3.3 Basics of cyber security; money-laundering and its prevention;

3.4 Security challenges and their management in border areas; linkages of organized crime with terrorism.

3.5 Various Security forces and agencies and their mandate

Note: The candidates are expected to be aware about the current developments related to the topics mentioned above.

---

5 TEMPLATES FOR 5 UNITS OF INTERNAL SECURITY

TEMPLATE 1: DEVELOPMENT-EXTREMISM LINKAGE

Mnemonic: DEPRIVED (Development-Economic-Political-Resource-Institutional-Vulnerability-Education-Displacement)

HEADING	SUB-HEADING	POINT	DATA & EXAMPLES
DEVELOPMENT DEFICIT	Backwardness	Regional disparity, Infrastructure gap	106 districts affected by LWE (2025); 90% in Scheduled Areas
	Basic Services	Health, Education, Connectivity	Literacy in Bastar (Chhattisgarh): 55% vs National 77.7%
ECONOMIC DEPRIVATION	Poverty & Unemployment	Lack of livelihood, Income inequality	45% population below poverty line in

			LWE areas vs 21% national average
	Land Alienation	Tribal land grabbed, Displacement	40% of displaced persons due to development projects are tribals
POLITICAL MARGINALIZATION	Governance Vacuum	Absent administration, Lack of representation	Only 8% Panchayats functional in core Naxal areas (Chhattisgarh)
	Voice Deficit	No participation, Ignored grievances	PESA (1996) implemented effectively in only 4 out of 10 scheduled states
RESOURCE EXPLOITATION	Mining & Forests	MNCs extracting, Locals not benefiting	80% of coal, 60% of bauxite in tribal areas; only 2-3% employed
	Environmental Damage	Deforestation, Pollution	Forest cover loss: 1.5 million hectares in mining areas (2015-2025)
INSTITUTIONAL FAILURE	Corruption	Siphoning of funds, Fake beneficiaries	Rs 50,000 crore leaked from MGNREGA in LWE states (CAG 2023)
	Law & Order Collapse	Police brutality, Fake encounters	1,800+ custodial deaths in LWE states (2020-2024) - NHRC data
VULNERABILITY EXPLOITATION	Identity Crisis	Tribal culture threatened, Mainstreaming forced	573 tribal languages endangered; 12 extinct since 2000
	Social Stratification	Caste discrimination, Class divide	SC/ST comprise 70% of Maoist cadre base
EDUCATION GAP	School Dropout	No schools, Poor quality	68% dropout rate at secondary level in LWE districts vs 36% national
	Skill Deficit	No vocational training, Youth unemployable	Only 15% youth in LWE areas have any skill training
DISPLACEMENT	Development Projects	Dams, Industries, Mining	60 million displaced since 1947; 40%

			tribals; 70% never rehabilitated
	Rehabilitation Failure	No land for land, Cash compensation useless	Only 30% of displaced received promised rehabilitation (2025 survey)

TEMPLATE 2: EXTERNAL & NON-STATE ACTORS

Mnemonic: PARTNERS (Pakistan-Adversaries-Radicalization-Terror-Networks-Espionage-Regional-Social Media)

HEADING	SUB-HEADING	POINT	DATA & EXAMPLES
PAKISTAN-SPONSORED TERRORISM	Terror Groups	LeT, JeM, HM operations	308 ceasefire violations (2024-2025); 47 infiltration attempts
	ISI Activities	Training camps, Funding, Handlers	127 terror training camps active in PoK (Intelligence inputs 2024)
ADVERSARIAL STATES	China	PLA incursions, Strategic encirclement	18 face-offs along LAC (2024); Doklam, Galwan legacy
	Bangladesh	Border issues, Illegal immigration	4,096 km porous border; 20 million illegal immigrants estimated
RADICALIZATION	Islamic Extremism	ISIS, Al-Qaeda modules	122 ISIS-inspired arrests (2020-2025); Kerala, Karnataka, UP modules
	Wahhabism Spread	Saudi funding, Madrasas	24,010 unregistered madrasas; ₹2,400 crore foreign funding
TERROR ORGANIZATIONS	Active Groups	LeT, JeM, NDFB, ULFA	106 banned organizations under UAPA
	Foreign Links	Pakistan, China, Myanmar bases	NSCN(IM) camps in Myanmar; ULFA in Bangladesh
NETWORKS	Sleeper Cells	Urban modules, Cyber cells	17 modules busted in 2023-24; Delhi, Mumbai, Hyderabad

	Hawala Channels	Money routing, Gold smuggling	₹15,000 crore annual hawala transactions estimated
ESPIONAGE	Intelligence Ops	Honey trapping, Data theft	156 espionage cases (2020-2024); Defence personnel targeted
	Cyber Espionage	State-sponsored hacking, APT groups	67 major cyber attacks attributed to China's APT groups (2023)
REGIONAL CONFLICTS	Nepal Maoists	Cross-border shelter, Arms supply	4 camps along India-Nepal border (Uttarakhand, UP, Bihar)
	Myanmar Insurgents	NSCN(K), ULFA camps	62 insurgent camps in Siang region (Myanmar)
SOCIAL MEDIA WARFARE	Propaganda	Fake news, Deepfakes, Misinformation	4.2 million fake accounts removed by MHA Fact Check Unit (2023)
	Recruitment	Online radicalization, Encrypted apps	78% ISIS recruits initially contacted via Telegram/Facebook

TEMPLATE 3: CYBER SECURITY & MONEY LAUNDERING

Mnemonic: CRIMINAL (Cyber-Ransomware-Identity-Money-Infrastructure-Networks-Assistance-Laws)

HEADING	SUB-HEADING	POINT	DATA & EXAMPLES
CYBER THREATS	Critical Infrastructure	Power grids, Railways, Airports	67 attacks on critical infra (2023); Mumbai power outage Oct 2020 suspected
	Data Breaches	Personal info, Financial data	75 million records leaked from Air India, IRCTC, Big Basket, Domino's
RANSOMWARE	Attacks	WannaCry, Maze, REvil variants	AIIMS Delhi (Nov 2022): 6 weeks shutdown, 40 million records compromised
	Crypto Payments	Bitcoin demands, Untraceable	₹1000 Plus crore ransom paid by Indian

			entities (2020-2025 est.)
IDENTITY CRIMES	Aadhaar Leaks	Database breaches, Ghost entries	210 million Aadhaar details on dark web (2023 report)
	Phishing	Banking frauds, OTP scams	₹1.25 lakh crore lost to cyber frauds (2022-23); 94,000 complaints/day
MONEY LAUNDERING	Hawala	Informal transfer, Terror funding	₹15,000-18,000 crore annual hawala transactions
	Shell Companies	Benami properties, Black money	3.20 lakh shell companies struck off (2017-2025)
INFRASTRUCTURE	Weak Systems	Outdated software, Unpatched vulnerabilities	68% government websites have security vulnerabilities (CERT-In audit)
	IoT Vulnerabilities	Smart devices, SCADA systems	23 million IoT devices in India; 89% unprotected
NETWORKS	Dark Web	Illegal marketplaces, Drugs, Arms	847 Indians arrested for dark web activities (2020-2024)
	Cryptocurrency	Untraceable transactions, Terror funding	₹44,700 crore crypto transactions flagged (2022-23)
INTERNATIONAL ASSISTANCE	MLA Treaties	Mutual Legal Assistance, Extradition	204 MLA requests pending with foreign countries (2023)
	Interpol Coordination	Red Corner Notices, Intelligence sharing	1,847 Red Corner Notices against Indians
LEGAL FRAMEWORK	IT Act 2000	Sections 66, 67, 69, 70	52,974 cases under IT Act (2023); conviction rate: 3.7%
	PMLA 2002	Money laundering prevention	5,422 cases registered; ₹9,870 crore attached

TEMPLATE 4: BORDER SECURITY & ORGANIZED CRIME

Mnemonic: BORDERS (Bangladesh-Operations-Riots-Drugs-Espionage-Routes-Smuggling)

HEADING	SUB-HEADING	POINT	DATA & EXAMPLES
BANGLADESH BORDER	Illegal Immigration	Rohingya influx, Demographic change	40,000+ Rohingyas; 20 million illegal immigrants (est.)
	Cattle Smuggling	₹5,000-8,000 crore annually	4,096 km porous border; 2.5 lakh cattle smuggled annually
OPERATIONS	Fencing	Smart fence, Tech integration	3,323 km fenced (81%); CIBMS pilot projects
	Surveillance	Drones, Night vision, Thermal imaging	450 drones deployed; facial recognition at 78 border checkpoints
REGIONAL TENSIONS	China LAC	Incursions, Infrastructure build-up	3,488 km LAC; 18 face-offs (2024); Chinese villages in Arunachal
	Pakistan LoC/IB	Infiltration, Ceasefire violations	308 violations (2025); 47 infiltration attempts
DRUG TRAFFICKING	Golden Crescent	Afghanistan-Pakistan-India route	₹72,000 crore worth drugs seized (2020-2025)
	Golden Triangle	Myanmar-India route	12,400 kg heroin seized from Manipur border (2023)
ESPIONAGE	Cross-border	ISI agents, Sleeper cells	127 espionage cases (2020-2025)
	Drone surveillance	Pak drones, Weapon dropping	187 drone sightings in J&K (2023); 9 shot down
SMUGGLING ROUTES	Arms	AK-47s, Pistols, Grenades	847 weapons seized at borders (2023)
	FICN	Fake currency notes	₹42.43 crore FICN seized (2023); Pakistan printing presses
CRIME-TERROR NEXUS	Funding	Drug money for terror operations	67% of LeT, JeM funding from drug trade
	Networks	D-Company, ISI, LeT collaboration	Ibrahim Dawood-ISI-LeT triangle; ₹500 crore annually

TEMPLATE 5: SECURITY FORCES & AGENCIES

Mnemonic: UNIFORMS (Unity-National-Intelligence-Forces-Operations-Reform-Modernization-Synergy)

HEADING	SUB-HEADING	POINT	DATA & EXAMPLES
UNITY OF COMMAND	Single Commander	Lack of coordination, Turf wars	26/11 Mumbai: NSG, Mumbai Police, Navy - no unified command
	Joint Operations	Assam Rifles + CRPF in NE; Army + BSF in J&K	Op Sunrise (Myanmar border): AR + Myanmar Army
NATIONAL INVESTIGATION AGENCY	Terror Cases	NIA Act 2008; 4th Schedule	1,876 cases registered; 312 ongoing (2025)
	Conviction	Success rate, Challenges	94.7% conviction rate; better than state agencies (32%)
INTELLIGENCE AGENCIES	Internal	IB, State intelligence, Special Branch	26 state intelligence bureaus; coordination via NATGRID
	External	RAW, NTRO, DIA	8 attaches abroad; limited HUMINT
CENTRAL ARMED POLICE FORCES	Paramilitary	CRPF, BSF, CISF, ITBP, SSB, NSG, Assam Rifles	10.5 lakh personnel; ₹1.15 lakh crore budget (2024-25)
	State Police	26.9 lakh personnel	144 police per lakh population vs UN standard 222
OPERATIONAL CHALLENGES	Equipment	Outdated weapons, Bullet-proof jackets shortage	50,000 BPJ shortage; 68% weapons beyond service life
	Training	Lack of counter-terror training, Human rights	Only 15% CAPF personnel trained in CBRN
REFORMS	Police Reforms	Prakash Singh judgment 2006	Only 8 states set up State Security Commissions
	Accountability	Human rights violations, Fake encounters	1,800+ custodial deaths (2020-2024)

MODERNIZATION	Technology	Drones, AI, Cyber capabilities	450 drones procured; NATGRID 40% operational
	Infrastructure	Smart borders, CIBMS, Surveillance	₹9,763 crore CIBMS; 78 facial recognition checkpoints
SYNERGY	Inter-Agency	NATGRID, NCTC (non-functional), MHA coordination	17 agencies under NATGRID; data sharing limited
	Center-State	Concurrent subject, political issues	J&K: Article 370 abrogation improved coordination

NOTE :

1). ONE TEMPLATE FOR WAY FORWARD IN THE LAST

2) PRACTICE QUESTIONS USING TEMPLATES IN THE LAST

PUNJAB PCS - INTERNAL SECURITY: COMPLETE PYQ ANALYSIS (2014-2020)

PAPER DETAILS

- **Paper:** General Studies Paper III
- **Total Paper Marks:** 250
- **Subject Analyzed:** Internal Security (Part of GS Paper III)
- **Years Analyzed:** 2014, 2015, 2018, 2020
- **Internal Security Questions:** 30 questions across 4 years

---

SYLLABUS MAPPING WITH PYQs

3.1 Linkages between development and spread of extremism

Questions Asked:

1. **2020 Q13** (15 marks) - Causes of violent extremism categorised into 'push' and 'pull' factors - individual and community factors
2. **2015 Q10** (15 marks) - Defence and development are complimentary but lack of development & economic reasons responsible for spread of extremism
3. **2014 Q10** (12 marks) - "There is not an iota of doubt that a definite linkage do prevail between development and spread of extremism"

3.2 Role of external, State and non-State actors in creating challenges to internal security

Sub-topics covered:

(A) External/State/Non-State Actors

1. **2020 Q14** (15 marks) - State sponsored cross-border terrorism, India's approach in context of neighbours
2. **2018 Q9** (15 marks) - China Pakistan Economic Corridor (CPEC) and implications on India's security
3. **2014 Q8** (12 marks) - Role of external, state and non-state actors in threatening national security

(B) Communication Networks and Media

1. **2018 Q12(a)** (10 marks) - Relationship between Media (print & electronic) and National Security
2. **2015 Q15(a)** (10 marks) - Role of Media in contemporary strategic environment
3. **2014 Q7** (12 marks) - Role of electronic media and social networking sites (positive and negative aspects)

(C) Social Networking Sites

1. **2015 Q11** (15 marks) - How Social Networking sites may affect India's security

---

3.3 Basics of cyber security; money-laundering and its prevention

(A) Cyber Security

1. **2020 Q12** (15 marks) - Dark Web, challenges to law enforcement agencies, counter measures to cyber terrorism
2. **2015 Q11** (15 marks) - Define Cyber security and Social Networking sites impact on security
3. **2014 Q19(a)** (7 marks) - Comprehensive cyber security policy is need of the hour

(B) Money Laundering

1. **2015 Q15(b)** (10 marks) - Role of Money Laundering as non-conventional threat
2. **2014 Q6** (12 marks) - International Banks/financial agencies in laundering black money, blanket ban solution?

3.4 Security challenges and their management in border areas; linkages of organized crime with terrorism

(A) Border Management

1. **2018 Q10** (15 marks) - Comprehensive Integrated Border Management System (CIBMS), challenges with Pakistan, Bangladesh, China borders
2. **2015 Q12** (15 marks) - Border Management in India - analytical account and methods of improvement
3. **2014 Q18(b)** (7 marks) - After 26/11, coastal security and management needs re-thinking
4. **2014 Q9** (12 marks) - Border state problems vs core state problems

(B) Organized Crime-Terrorism Linkage

1. **2018 Q11(a)** (10 marks) - Narco-Drug trafficking as threat to internal security with special reference to Punjab

---

3.5 Various Security forces and agencies and their mandate

Questions Asked:

1. **2015 Q13** (15 marks) - Organization and role of National Security Guards (NSG), deployment in recent months
2. **2014 Q19(b)** (7 marks) - Biggest paramilitary force, its mandate and special features

---

ADDITIONAL TOPICS (Not explicitly in syllabus but related)

(A) Police Reforms

1. **2020 Q11** (15 marks) - Reforms in Police as bottleneck in internal security policy

(B) Types of Terrorism/Security Challenges

1. **2018 Q11(b)** (10 marks) - Hologrammatic Terrorism and asymmetric war
2. **2015 Q14(a)** (10 marks) - Separatism in Jammu & Kashmir
3. **2015 Q14(b)** (10 marks) - Left Wing Extremism (LWE)
4. **2014 Q18(a)** (7 marks) - 'As Iraq Burns, World Feels the Heat' - implications for India

(C) Comprehensive Security

1. **2018 Q12(b)** (10 marks) - Comprehensive security vs conventional security paradigm

---

LINKAGES BETWEEN DEVELOPMENT AND SPREAD OF EXTREMISM

UPSC Previous Year Questions

• 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)

Linkages between development and the spread of extremism

Extremism can be defined as any ideology considered to be far outside the mainstream attitudes of a society or to violate common moral standards. It means an ideology deflected from the mainstream of common moral standards, which can be perceived as good or bad depending upon the political and philosophical values.

The linkage between development and extremism is intricate: **underdevelopment fuels alienation, poverty, and injustice**, creating fertile ground for extremist ideologies, as seen in Naxalism or Boko Haram. Conversely, **equitable development in education, employment, and infrastructure** can mitigate these risks by fostering inclusion and stability.

Extremism – Forms

Form	Definition	Key Characteristics	Examples
Religious Extremism	Violent defence of religious identity based on political interpretation.	Advocates fundamentalism; targets perceived threats to religion.	Pakistan's Hizbul Mujahideen, ISIS.
Left-Wing Extremism (Naxalism)	Anti-capitalist ideology seeks to end state violence through violence.	Focus on Maoist ideology, guerrilla warfare, and rural mobilisation.	CPI (Maoist) in the Red Corridor; Naxalbari uprising.
Ethnic Extremism	Belief that one's ethnic group is superior to others and should have dominance or exclusive rights—politically, culturally, or territorially.	Intense allegiance to one's ethnic group, dominance over others, and conflict incitement.	Manipur Violence of 2023.
Terrorism	Use of violence to instil fear, aligned with extremist ideologies.	Includes cyber terrorism, lone wolf attacks, and state-sponsored acts.	26/11 Mumbai attacks; ISIL-inspired attacks.

---

1. Challenges in Development Leading to Extremism

Developmental Challenge	Mechanism Fueling Extremism	Examples
1. Economic Deprivation and Unemployment	Widespread poverty and lack of employment opportunities create desperation, driving youth to join	In **Jammu & Kashmir**, youth unemployment (over 20% in

	extremist groups (religious, ethnic, or leftist) for financial incentives or ideological appeal.	2023) fuels recruitment for politico-religious militancy.
2. Educational Backwardness	**Low literacy and limited access to quality education enable radicalisation** through misinformation, making populations vulnerable to extremist propaganda across ideologies.	**Remote NE districts** like rural Arunachal Pradesh report literacy rates as low as 45–65% well below the national average (80.9%), aiding extremist recruitment.
3. Perceived Socio-Economic Injustice	**Inequitable resource distribution and land alienation** foster resentment, positioning extremists as champions of justice for marginalised communities, including religious or ethnic groups.	In **Assam**, perceived neglect of indigenous **Bodo communities** drives ethnic extremism, exemplified by **Bodo–Muslim clashes (2012)**.
4. Governance Vacuum	**Absence of effective public services** enables extremist outfits to establish parallel systems, gaining legitimacy among underserved populations.	**Maoists run "Jan Adalats"** in LWE areas.
5. Social Marginalisation	**Historical exclusion of communities from mainstream opportunities** breeds alienation, making them receptive to anti-state narratives from religious, ethnic separatists, or left-wing groups.	In **Punjab**, socio-economic marginalisation of Sikh youth in the 1980s fueled the **Khalistan movement's separatist agenda.**
6. Weak Forest Rights Implementation	**Poor enforcement of Forest Rights Act (FRA)** and the **PESA Act** denies tribals autonomy, making them vulnerable to extremist propaganda.	In **Gadchiroli (Maharashtra)**, unsettled forest rights claims drive tribal protests, aiding Naxal recruitment.

2. Impact of Extremism on Development

Impact Area	Consequences	Examples
1. Economic Disruption	**Extremist attacks disrupt infrastructure and investment**, leading to reduced FDI, stalled projects, and economic losses.	**Oil pipelines** are often blown up by insurgents, tea gardens are targeted for extortion.
2. Social Instability	**Violence creates fear**, displaces communities, and causes a breakdown of **social cohesion**, resulting in migration from affected areas.	**Red Corridor villages** face displacement due to Maoist violence.

3. Governance Challenges	**Extremists target government institutions**, undermining authority, **weakening the rule of law**, and delaying development projects.	**"No-go" zones in Jharkhand's Bastar region** hinder state presence and development initiatives.
4. Human Capital Loss	**Loss of lives and brain drain** due to violence reduce the workforce and hamper **skill development.**	**Deaths of more than 4000 civilians and 2500 security force personnel since the 2000s.**
5. Environmental Degradation	**Extremists exploit natural resources** for funding, causing deforestation and resource depletion that harm sustainability.	**Maoist extortion in Odisha** forests impacts tribal livelihoods.

3. Government Strategies to Counter Extremism

Strategy	Initiatives and Measures	Impact
1. Security-Centric Measures	Implementation of **Operation Green Hunt**, **SAMADHAN doctrine**, deployment of **Central Armed Police Forces (CAPF)**, and adoption of **Andhra Pradesh's Greyhound Model** for targeted anti-insurgency operations.	Achieved a **76% reduction in LWE violence (2013–2023)**; CoBRA units effectively disrupted Maoist networks in the Red Corridor.
2. Development-Oriented Interventions	Execution of **Aspirational Districts Programme**, **Saranda Development Plan**, **PM GatiShakti** for infrastructure connectivity, and **PM DEVINE** to foster holistic development in North-East India.	Covered **35 LWE districts** under Aspirational Districts; constructed **10,600 km of roads** in Red Corridor (2014–2023).
3. Rights-Based Empowerment	**Enforcement of the Forest Rights Act (FRA)**, implementation of the **PESA Act**, formation of **Self-Help Groups (SHGs)**, and provision of tribal rehabilitation packages to ensure inclusive growth.	**Distributed 1.9 million FRA titles; implemented PESA in 10 states**, enhancing tribal autonomy and participation.
4. Rehabilitation and Reintegration	**Execution of the Surrender and Rehabilitation Policy**, offering financial assistance, housing, and vocational training to reintegrate former extremists into society.	**Chhattisgarh approved 15,000 houses under PM Gramin Awas Yojana** to rehabilitate surrendered Maoists and victims of Maoist violence, marking a major rehabilitation initiative.
5. Technological Advancements	**Utilisation of UAVs for surveillance**, **NTRO** for intelligence gathering, **LWE Mobile Tower Project** for	Installed **2,335 mobile towers** in LWE areas; operationalised **NATGRID since 2020** for **real-time intelligence sharing.**

	connectivity, and **MCTNS** and **NATGRID** for enhanced security coordination.	
6. Community Engagement	Promotion of the **Civic Action Programme (CRPF-run schools, medical camps)** and **BSF's "Winning Hearts and Minds" initiative** to build trust through skill training, medical camps, and healthcare initiatives.	Reached **10,430 cases in J&K through CAP (2023)**; facilitated trust-building via medical camps and healthcare programs in LWE regions.

4. Way Forward

Strategy	Recommendation
1. Holistic Governance and Security Synergy	**Integrate security operations** with development initiatives to address root causes, **enhancing governance for sustainable peace**, as recommended by the **2nd ARC (2008).**
2. Terrain-Specific Security Enhancements	**Deploy localised, terrain-trained police forces** to reduce reliance on Army operations, improving agility, as suggested by the **Shekatkar Committee.**
3. Tribal Economic Empowerment	**Ensure full implementation of PESA and FRA** to secure economic benefits for tribals from forest resources, as advocated by **Nandan Nilekani in *Imagining India.***
4. Building Inclusive Institutions	**Tackle poverty and promote counter-narratives to extremist ideologies**, fostering inclusive governance, as outlined in the **UN Plan of Action (2016).**
5. Digital Counter-Propaganda Efforts	**Collaborate with tech platforms** to curb online radicalisation and extremist content, as proposed by the **Christchurch Call (2019)** — *India is not a signatory.*
6. Cooperative Federalism and Technological Innovation	**Strengthen Centre–State coordination** and **leverage AI-driven intelligence for security**, inspired by **Chhattisgarh's Unified Command model.**

The **development–extremism nexus** necessitates a balanced approach, integrating security, inclusive growth, and community trust. **Empowering tribals, enhancing governance, and countering radicalisation** are pivotal for sustainable peace and development.

Left Wing Extremism in India

Left-Wing Extremism (LWE) refers to **violent insurgency** driven by **Maoist or Naxalite ideologies**, primarily targeting **marginalised regions**. It stems from **socio-economic**

inequalities, land disputes, tribal neglect, corruption, human rights violations, and the ideological appeal of **revolutionary justice.**

Naxalism originated in **Naxalbari, W.Bengal, 1967**, with a **peasant uprising**. LWE was a response to **deep-seated social and economic injustices**, particularly in rural areas. Over the years, left-wing extremism has evolved and **spread to several states**, aiming to **overthrow the government** and establish a **communist society.**
The goal is the **overthrow of the Indian state and establishment of a "people's government"** along Maoist lines.

UPSC Previous Year Questions

1. Naxalism is a social, economic, and developmental issue manifesting violent internal security threats. In this context, discuss the emerging issues and suggest a multilayered strategy to tackle the menace of Naxalism. **(2022)**
2. What are the 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? **(2020)**
3. 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. **(2018)**
4. 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. **(2015)**
5. Article 244 of the Indian Constitution relates to the administration of scheduled areas and tribal areas. Analyse the impact of non-implementation of the provisions of the Fifth Schedule on the rise of Left Wing Extremism in India.

Evolution of LWE

Naxalbari (1967–72)	Post-Charu Phase (1970s–2000)	CPI (Maoist) Era (2004–Now)	Current Trends (2020s)
Sparked by agrarian unrest, aimed at land redistribution through armed struggle.	After Charu Majumdar's death, the movement split into PWG and MCC; expanded to Bihar and Andhra Pradesh.	PWG and MCC merged to form CPI (Maoist); PLGA was created, increased urban reach and guerilla tactics.	Violence declined, but covert urban Naxal networks and targeted attacks persist in some core districts.

Present Status of Left Wing Extremism in India

Overall Status	Affected Districts	Most Affected Districts	Violence Trends
LWE declining: 38 districts affected in 2024, with goal to eradicate by March 2026.	Dropped from 126 (2018) to 38 (2024) due to effective counter-insurgency measures.	Reduced from 12 to 6; 4 in Chhattisgarh, 1 each in Jharkhand, Maharashtra.	81% drop in incidents (1,915 in 2010 to 374 in 2024); 85% fewer deaths.

Surrenders	Government Commitment	Financial Support
Over 8,000 Naxalites surrendered in last decade, reintegrating via rehabilitation.	Aims to eliminate LWE by March 31, 2026, via security and development focus.	Special Central Assistance (SCA) scheme: ₹30 crore for the most affected, ₹10 crore for concerned districts.

---

1. Causes of Left-Wing Extremism in India

Cause	Description	Example
1. Land Dispossession & Forest Rights	Failure to implement land reforms and Forest Rights Act (FRA), **depriving tribals of ancestral land and resources.**	**Only 12% of tribal land claims were approved in Jharkhand** (2023 Tribal Affairs Ministry Report).
2. Socio-Economic Deprivation	**Chronic poverty, unemployment, and lack of healthcare/education** in remote tribal regions.	**90% of Sukma (Chhattisgarh)** lacks access to secondary education (NITI Aayog 2023).
3. Governance Deficits & Corruption	Corruption in welfare schemes and **absence of local administration in conflict zones.**	**PDS leakages in Bastar:** 40% ration diverted to black markets (CAG 2022).
4. Exploitation by Middlemen	**Tribal communities are cheated in minor forest produce trade** by contractors and intermediaries.	**Tendu leaf collectors paid ₹32/kg in Odisha vs market rate ₹50/kg** (ED Report 2024).
5. Ideological Radicalization	Maoist propaganda **exploits alienation**, promising **egalitarian revolution and tribal justice.**	**Surrendered cadres cite "broken promises"** as a recruitment tactic (Chhattisgarh Police 2024).

Incidents of Violence by Left-Wing Extremism in India

CIVILIANS KILLED BY LWE	INCIDENTS OF ATTACK ON ECONOMIC INFRASTRUCTURE
2010 – 720 2014 – 222 2024 – 121	2010 – 400 2014 – 365 2024 – 25

2. Challenges Ahead in Combating Left-Wing Extremism

Challenge	Description	Example
1. Geographical & Terrain Barriers	**Dense forests and rugged terrain** in LWE zones hinder security operations and **infrastructure development.**	**Abhujmad (Chhattisgarh):** 4,000 sq km of uncharted forest serves as a Maoist stronghold.
2. Tribal Sympathy & Grievances	Maoists exploit **land displacement, governance gaps, and social exclusion** to retain tribal support.	**Bastar region:** 60% of displaced tribals denied compensation (NHRC 2023).
3. Urban Underground Networks	**Covert urban cells** in cities like Mumbai, Delhi, fundraise, recruit, and **spread propaganda via digital platforms.**	**NIA busted the Delhi module** recruiting students from JNU and Jamia.
4. Intelligence & Coordination Gaps	Poor inter-agency coordination and limited tech adoption **weaken real-time threat response.**	Only **15% of LWE police stations use AI/ML tools** (MHA 2024).
5. Security & Development Lapses	**Resurgence risk** due to gaps in governance, delayed welfare schemes, or reduced security pressure.	**2026 Deadline:** MHA's target to eliminate LWE faces hurdles in Odisha's Koraput district.

3. Factors that Sustain Left Wing Extremism

Factor	Description	Example
1. Ideological Appeal	Maoist propaganda exploits tribal alienation, promising land, forest, and water rights through revolution.	**"Jal, Jungle, Jameen" campaigns** mobilised tribal support in Odisha.
2. Organizational Strength	**Cadre-based hierarchy**, local leadership, and efficient logistics enable sustained operations in remote areas.	**People's Liberation Guerrilla Army (PLGA)**, with 8,000–9,000 fighters (60% female), uses seized weapons like INSAS rifles, active in Jharkhand, Andhra Pradesh.

3. Governance Deficits	**Poor implementation of FRA/PESA** and corruption in welfare schemes deepen alienation.	**Only 12% of tribal land claims approved in Jharkhand** (Tribal Affairs Ministry, 2023).
4. Cross-Border Networks	**Arms trafficking via Myanmar** and alliances with NE insurgent groups sustain logistics.	**NSCN-K supplied AK-47s to Maoists in Chhattisgarh** (NIA, 2024).
5. Technological Adaptation	Use of **encrypted apps (Telegram)** and drones for coordination and surveillance.	Naxalites use private Telegram chats to plan ambushes, like the **2021 Sukma-Bijapur attack in Chhattisgarh.**

4. Government Measures Against Left-Wing Extremism

Measure	Description
1. SAMADHAN Doctrine	Multi-pronged strategy combining **security, development, rights, governance, and perception management** to counter LWE.
2. Operation Black Forest	Operation Black Forest, a **21-day joint operation** between the CRPF and Chhattisgarh Police, marked the **longest continuous anti-Naxal campaign**, resulting in the deaths of 27 Naxals, including top leader **Nambala Keshav Rao**, in the Abhujmad region.
3. Greyhounds & COBRA Forces	**Elite commando units** specialising in jungle warfare, counter-guerrilla tactics, and rapid response in LWE zones.
4. Surrender & Rehabilitation	**Financial aid (₹10,000/month)**, vocational training, and land allocation to reintegrate cadres into mainstream society.
5. Critical Infrastructure Push	**Roads (8,175 km)**, mobile towers (2,335), and **BharatNet** to improve connectivity and security in LWE-affected areas.
6. PESA & FRA Implementation	**Tribal self-governance via Gram Sabhas** to address land rights, forest resources, and alienation.
7. Security-Related Expenditure	**Central funds for modernising state police**, fortifying stations, and community policing in high-risk districts.
8. Naxal Surrender Policy 2025	Guarantees **rehabilitation within 120 days**, urban housing, and agricultural land for surrendered cadres.
9. Tech-Driven Surveillance	**AI, drones, and blockchain** deployed for predictive policing, fund tracking, and real-time intelligence. *Example:* **Andhra Pradesh's CRIME Analytics Platform** reduced IED attacks by **40%.**
10. Aspirational Districts Program	Focused development in the **30 most LWE-affected districts** to address poverty, education, and healthcare gaps.
11. National Policy (2015)	Holistic approach with **security, development, and tribal rights** to shrink LWE's geographical spread. *Example:* **LWE districts reduced from 126 (2010) to 38 (2024);** violence down by **81%.**

SAMADHAN: Strategy for Conflict Resolution

Letter	Meaning	Explanation
S	Smart Leadership	Smartly deal with the situation
A	Aggressive Strategy	Avoid confrontation
M	Motivation and Training	Motivate to join the mainstream
A	Actionable Intelligence	Assert government authority
D	Dashboard-Based KPIs	Develop confidence among stakeholders
H	Harness Technology	Hit the problem hard (tactically)
A	Action Plan for Each Theatre	Appoint interlocutors
N	No Access to Financing	Negotiate with credible leaders

5. Left Wing Extremism – Way Ahead

Measure	Description
1. Community-Led Governance	Integrate local tribals in administration and **leverage civil society to bridge trust deficits and foster grassroots participation.**
2. Counter-Ideological Campaigns	**Promote constitutional democracy** through education, workshops, and media to counter Maoist propaganda and radicalisation.
3. Strengthened Centre-State Coordination	Synchronized strategies with **clear role delineation**, joint task forces, and **real-time intelligence sharing.**
4. Modernized Security Infrastructure	**Equip forces with drones, GIS, and AI** for precision strikes, camp mapping, and IED detection in dense forests.
5. Fast-Track Tribal Rights	Accelerate **FRA/PESA implementation** to resolve land disputes and ensure tribal ownership of forest resources.
6. Socio-Economic Inclusion	Expand the **Aspirational Districts Program** to address poverty, healthcare, and skill gaps in LWE-affected regions.

Left Wing Extremism (LWE) in India represents a **multifaceted internal security challenge**, deeply entrenched in **historical injustices, socio-economic inequalities,** and the persistent **marginalisation of tribal communities.** Despite commendable achievements in curbing violence, the road to lasting peace lies not in force alone, but in a **holistic strategy** that combines **inclusive development, effective governance, and meaningful empowerment.**
Realising India's target of **eliminating Left Wing Extremism by March 31, 2026**, requires sustained efforts to address root causes and promote a better ideology, as it is said —

"You cannot defeat an ideology with force, only with a better ideology."

Militancy in Jammu and Kashmir

Militancy in Jammu and Kashmir (J&K) is a **prolonged internal security challenge**, shaped by a mix of historical discontent, political betrayal, cross-border terrorism, and socio-economic exclusion. Since the late 1980s, the region has witnessed a **transition from civil unrest to full-scale asymmetric warfare**, often fueled by **proxy actors and external state support**, primarily from Pakistan.

According to Ajit Doval, India's National Security Advisor, tackling such non-conventional threats requires shifting from a reactive to a proactive **"Defensive–Offensive"** doctrine, combining deterrence, precision strikes, and strategic psychological warfare. His 4D strategy – **Deter, Detect, Disrupt, Destroy** – has guided much of India's counter-terror approach post-2016, especially in Kashmir.

UPSC Previous Year Question

1. Winning of Hearts and Minds in terrorism-affected areas is an essential step in restoring the trust of the population. Discuss the measures adopted by the Government in this respect as part of the conflict resolution in Jammu and Kashmir. **(2023)**
2. The banning of 'Jamaat-e-Islami' in Jammu and Kashmir brought into focus the role of over-ground workers (OGWs) in assisting terrorist organisations. Examine the role played by OGWs in assisting terrorist organisations in insurgency-affected areas. Discuss measures to neutralise the influence of OGWs. **(2019)**

Evolution of Militancy in Kashmir

Pre-1947	Post-1947 Wars	Militancy Era	2010–2025
• Political marginalisation under Dogra rule • Discontent among the Muslim majority • Rise of Sheikh Abdullah and National Conference	• Accession of J&K to India (1947) • First Indo-Pak war (1947–48) and creation of PoK • Wars in 1965 and 1971 over Kashmir	• Rise of armed insurgency (from 1989) • Foreign training and infiltration by Pakistan-based groups • Mass exodus of Kashmiri Pandits (1990)	• High-profile attacks (Uri, Pulwama 2019, Pahalgam 2025) • Abrogation of Article 370 (2019) • Shift to hybrid warfare involving propaganda and cyber threats • Pahalgam Terror Attack

---

1. Factors Responsible for Militancy in J&K

Factor	Description	Example
1. Political Grievances	Perceived **betrayal of promised autonomy** under Article 370 and **allegations of electoral manipulation** fuel unrest.	*The 1987 rigged elections crushed Muslim United Front*, triggering widespread alienation.
2. External Interference	**Pakistan's ISI provides arms, training, and financial support** to militant groups, sustaining insurgency.	*The 1999 Kargil War* involved Pakistani infiltrators occupying Indian territory.
3. Socio-Economic Gaps	**High unemployment, poor infrastructure, and lack of development** create fertile ground for militancy recruitment.	*J&K's unemployment rate at 18.3% in 2023*; only 35% youth employed in Kupwara (NSSO 2023).
4. Ideological Radicalization	Rise of Islamist groups like **Hizbul Mujahideen**, spreading radical ideology and mobilizing youth.	*Burhan Wani's 2016 killing* sparked mass protests and surge in militant recruitment.
5. Governance Deficit	Corruption, bureaucratic apathy, and **delayed justice** erode public trust and exacerbate alienation.	*AFSPA:* Over 4,000 human rights violation complaints filed from 2010–2016 (J&K SHRC).
6. Demographic & Communal Tensions	Ethnic and religious divisions are exploited to **deepen mistrust and polarise communities.**	*The 1990 exodus of 90,000+ Kashmiri Pandits* altered the valley's demographic composition.
7. Political Instability	Frequent changes in governance and the **absence of elected governments** create power vacuums exploited by militants.	*Since the 1990s, there have been multiple instances of both President's Rule and Governor's Rule* in J&K.

---

2. Role of Over-Ground Workers in J&K Militancy

Over-Ground Workers (OGWs) are individuals who, while **not directly involved in armed attacks or militancy**, provide crucial logistical, financial, intelligence, and ideological support to terrorist or insurgent groups. They operate covertly within civilian populations, often blending into society, and play a vital role in **sustaining and expanding militant operations** by aiding recruitment, spreading propaganda, and facilitating communication between active militants and their handlers.

Role Name	Description	Measures to Counter OGWs
1. Intelligence Gathering	OGWs supply precise local intelligence to terrorists, enabling ambushes and aiding escape during military operations.	Conduct **intelligence-based operations** like *Operation All Out* to identify and arrest OGW networks.

2. Logistics Support	They provide militants with **shelter, transport, arms, and hideouts**, critical for long-term survival and mobility.	Implement **area surveillance, crack communication channels**, and monitor suspect properties and assets.
3. Spreading Propaganda	OGWs **promote separatist ideologies** via social media, mosques, and gatherings to radicalise local populations.	Launch **counter-narratives** like *Operation Dreams* and **de-radicalisation campaigns** targeting youth.
4. Recruitment	OGWs **target vulnerable youth** for recruitment, exploiting unemployment and grievances to lure them into terror.	**Community policing and youth engagement programs** like *Himayat* and *UMEED* to channel youth productively.
5. Fundraising	They **collect funds under fake charities** or events and funnel them to militant organisations and sleeper cells.	Use **UAPA and financial tracking tools** (FATF compliance, ED raids) to curb terror financing.
6. Creating Public Disorder	OGWs **provoke stone-pelting, riots, and protests** to divert security forces and protect militants during operations.	Deploy **riot control teams**, enforce *Section 144*, and run awareness drives on OGW manipulation tactics.

3. Impact of Jammu & Kashmir Militancy

Impact	Description	Example
1. Human Losses	Thousands of civilians, security personnel, and militants were killed, creating a cycle of **violence and trauma.**	*Over 40,000 deaths have occurred since 1990* (Ministry of Home Affairs, 2023).
2. Economic Disruption	Tourism and local businesses suffer due to instability, hampering **J&K's economic growth.**	*J&K's tourism revenue significantly dropped by nearly 60% in 2019* due to unrest.
3. Social Polarization	Communal tensions and an **exodus of Kashmiri Pandits** fractured social cohesion.	*Over about 70,000 Pandit families* have been displaced so far.
4. Security Burden	Heavy deployment of forces strains resources and escalates tensions, leading to **militarised civilian spaces** and human rights allegations.	*According to MHA (2024)*, the Army maintains a strength of around *1.3 lakh personnel*, 80,000 deployed on the border.
5. Psychological Impact	Fear and mistrust among locals and security forces hinder **peace-building and normalcy.**	*Mental health issues, including PTSD*, are significantly prevalent in Kashmir Valley.

6. Infrastructure Stagnation	Chronic underdevelopment due to **diverted funds from welfare to counter-insurgency operations.**	*CAG Report:* Only **60% of PMDP projects** were completed in J&K.

4. Initiatives by the Government

Initiative	Description
1. Article 370 Abrogation (2019)	Revoked special status to integrate J&K fully with India, aiming to **curb separatism and boost development.** **J&K Reorganisation Act, 2019** led to empowerment of people, removal of discriminatory laws, and integration of the region into the mainstream.
2. Strengthened Anti-Terror Laws	**UAPA (2019) amendments** empower NIA to seize assets and designate individuals as terrorists. In 2022, **J&K had the highest number of UAPA cases** in India (371 cases).
3. Operation All Out	Security forces' targeted campaign to **neutralise militants**, disrupting terror networks.
4. Development Schemes	**PM's Development Package (2015)** and **Aspirational Districts Programme** focus on infrastructure and jobs. ₹80,000 crore allocated for J&K.
5. Civic Action Programmes	**CRPF's "Winning Hearts and Minds"** initiative builds trust through schools and healthcare. CRPF built **50+ schools** in J&K.
6. UDAAN Scheme	**Special Industry Initiative (SII)** to enhance employability of youth by providing skill development and exposure to corporate India. Udaan and allied initiatives have trained and employed thousands of youth.
7. Kashmiri Saffron GI Tag (2020)	**Kashmiri saffron** received a **GI tag**, boosting global recognition and leading to a **20% rise in exports** by 2023.
8. Youth and Community Programs	Initiatives like **Project Himayat, Nai Manzil, USTAAD, Project Sadbhavana, Project Umeed, Parvaaz Scheme, and Village Defence Groups** empower youth and promote social inclusion.

5. Soft Counter Approaches: Winning of "Hearts and Minds"

The conflict-ridden region of Jammu and Kashmir has seen numerous efforts to restore peace and stability.
A key approach is the **"Hearts and Minds" strategy**, focusing on **rebuilding trust and fostering peaceful coexistence** by engaging directly with local communities.

Approach	Description	Example

1. Community Building	Initiatives fostering **trust through education, healthcare, and women's empowerment** in conflict zones.	*Operation Sadbhavana* by the Indian Army promotes civilian welfare in J&K and Ladakh.
2. Rehabilitation of Militants	Creating a **Surrender & Reintegration Framework** offering vocational training and financial support.	*Surrender and rehabilitation policies* provide stipends and job assistance.
3. Infrastructure Development	**Bridging rural–urban gaps** by improving connectivity and access to services.	*PMGSY built 2,500 km of roads* in J&K (2020–2024).
4. Healthcare Initiatives	Establishing **advanced medical facilities** to reduce healthcare disparities.	*AIIMS Vijaypur* has treated over *1.6 lakh patients.*
5. Community Dialogues	Direct engagement between officials and locals to **address grievances and ensure inclusive governance.**	*Back to Village* programme enhances public–government interface.
6. Youth Engagement	Channelising youth energy into **sports and skill-building** to deter radicalisation.	*Khelo India* has created *50+ sports complexes* across the country.
7. Positive Media Narratives	**Counter extremist propaganda** by promoting local culture and unity.	*Radio Sharda*, a community radio station in Jammu, broadcasts in Kashmiri and Dogri.
8. Connectivity Initiatives	**Enhancing digital and physical integration** to mainstream development.	*BharatNet's 1,200+ gram panchayats* connected with high-speed internet.

6. Way Forward

Measure	Description
1. Inclusive Governance	**Strengthen local governance** and ensure transparent elections. *District Development Council (DDC)* polls saw 51% voter turnout.
2. Deradicalization Programmes	Promote **education, counselling, and community engagement** to deter youth militancy.
3. Economic Development	Create **jobs and skill development programmes** to reduce unemployment and militant recruitment. In 2025, *Skill India initiatives* trained *10,000 youth* in J&K.
4. Security Reforms	**Balance AFSPA with human rights**—embrace *Doctrine of Restraint* (D.S. Hooda) for measured use.
5. Regional Cooperation	Engage Pakistan and neighbours to **curb cross-border terrorism and arms smuggling.** Strengthen *SAARC framework for counter-terrorism* under the

	1987 Regional Convention on Suppression of Terrorism and its **2004 Additional Protocol.**

Militancy in Jammu and Kashmir is a complex issue rooted in **historical grievances, external interference, and socio-political alienation.**
While security measures have reduced violence post-2019, sustainable peace requires addressing **governance deficits, inclusive development, and youth empowerment.** Initiatives like *youth engagement, cultural preservation, and regional diplomacy* are essential for long-term peace.

As former PM Atal Bihari Vajpayee noted, **"Insaniyat (humanity), Jamhooriyat (democracy), and Kashmiriyat (Kashmir's ethos)"** must guide long-term solutions.

North-East Insurgency

The North-East region of India, often referred to as the **'Ashtalakshmi'** of India due to its **eight states symbolising prosperity and diversity**, holds immense **cultural richness and strategic significance.** Despite this, it has long been afflicted by insurgency. Since the 1950s, the region has witnessed violent separatist movements and autonomy struggles, fueled by **historical marginalisation, ethnic tensions, demographic shifts, and cross-border infiltration.** Experts like **Sanjib Baruah**, author of *In the Name of the Nation*, argue that the region's complex colonial legacy and post-independence governance failures have entrenched a sense of alienation, sustaining insurgencies.

While peace accords (such as the **Mizo Accord**, **Bodo Agreement**) and development initiatives have reduced armed conflict in states like **Mizoram** and **Tripura**, unresolved grievances around **indigenous identity, economic underdevelopment, and external support** (from groups in Myanmar or Bangladesh) continue to hinder sustainable peace and mainstream integration.

UPSC Previous Year Question

1. Cross-border movement of insurgents is only one of the several security challenges facing the policing of the border in North-East India. Examine the various challenges currently emanating across the India–Myanmar border. Also, discuss the steps to counter the challenges. **(2019)**
2. The North-Eastern region of India has been infested with insurgency for a very long time. Analyse the major reasons for the survival of armed insurgency in this region. **(2017)**
3. 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. **(2015)**

Historical Background of North-East Insurgency

Pre-Independence	Post-Independence (1947–1960s)	1970s–1980s	1990s–2000s	2010s–Present
• Ethnic and tribal groups (Nagas, Mizos) resisted British colonial rule, seeking autonomy. • Limited integration with mainland India due to geographic and cultural isolation.	• Naga insurgency began with demands for independence (Naga National Council, 1947). • Mizo rebellion (1966) sought self-rule. • Central government used military measures and promised statehood.	• Rise of multiple insurgent groups (such as ULFA in Assam, 1979). • Demands for sovereignty, ethnic rights, and resource control. • Insurgencies fueled by economic neglect and ethnic tensions. • Peace accords attempted (Mizo Accord, 1986).	• Proliferation of smaller militant groups. • Cross-border support from neighbouring countries. • Ceasefires and peace talks initiated (NSCN-IM, 1997) amid ongoing violence. • Economic development initiatives introduced to curb unrest.	• Decline in violence due to counter-insurgency, peace agreements, and development programs. • Some groups (ULFA factions) signed accords. • Residual low-level militancy persists in Manipur and Nagaland.

---

1. Reasons for Insurgency in North-East

Reason	Description	Example
1. Ethnic Identity Assertion	Over **200 tribes** seek to preserve distinct identities, resisting assimilation and demanding cultural and political autonomy.	**NSCN (IM)** demands *"Greater Nagalim,"* uniting Naga-inhabited areas across three states.
2. Economic Underdevelopment	Poor infrastructure, unemployment, and slow growth led to frustration and easy recruitment by insurgent groups.	Several NE states' **per capita income** is below the national average, though *Mizoram performs better.*
3. Political Alienation & Exclusion	Perceived neglect, **lack of representation, and**	*Assam Movement (1979–85)* against illegal migrants

	centralisation led to separatist sentiments and autonomy demands, giving rise to *"durable disorder,"* as per Sanjib Baruah.	and political marginalisation.
4. External Support & Cross-Border Linkages	**Cross-border sanctuaries, arms, and training** from Myanmar, Bangladesh, and China sustained insurgent groups and violence.	**ULFA, NSCN (K)** camps in Myanmar; Bangladesh handed over top ULFA leaders (2009–15).
5. Governance Deficit & Corruption	**Corruption, slow justice, and weak state capacity** eroded faith in government, fueling local grievances and extortion.	Extortion by insurgents, **slow peace accord implementation**, and **AFSPA** alienated Naga people.

2. State-wise Insurgency: Causes and Measures

A. Assam

Aspect	Details
1. Insurgency	Militancy led by **ULFA**, **NDFB**, and **Karbi groups** like KNLF seek autonomy or separatism. Post-2010 violence declined due to peace talks.
2. Causes	**Ethnic strife** among Bodos, Assamese, and Bengali migrants, fueled by **illegal immigration** from Bangladesh; **socio-economic disparities** and unemployment drive militancy.
3. Measures Taken	**Assam Accord (1985)** addressed illegal immigration; **Bodo Peace Accord (2020)** granted autonomy. **Operation Bajrang (1990–91)** neutralised ULFA networks. **PM-DevINE and PM GatiShakti** enhanced socio-economic integration.

B. Nagaland

Aspect	Details
1. Insurgency	The **NSCN (IM)** pursues a **sovereign Nagalim**, fueling separatist militancy. Ceasefires since 1997 have reduced violence, though factionalism persists.
2. Causes	**Deep-rooted Naga nationalism** from historical isolation; **cross-border support** from Myanmar and China; governance gaps sustain unrest.
3. Measures Taken	**Naga Peace Accord (2015)** advanced reconciliation; **Aspirational District Programme** built infrastructure and trust.

C. Manipur

Aspect	Details
1. Insurgency	**Meitei groups (UNLF, PLA)** and **Kuki–Zomi militias** fuel ethnic strife and anti-state militancy; **drug trafficking** and extortion destabilise the state.
2. Causes	**Ethnic rivalries**, particularly Meitei–Kuki clashes; **poverty and unemployment**; porous **Indo–Myanmar border** allows smuggling.

3. Measures Taken	**AFSPA deployment** supports counter-insurgency. **CRPF's Winning Hearts and Minds initiative** fosters civic engagement and reconciliation.

D. Manipur Violence 2023

Dimension	Key Details & Examples
1. Historical Background	Long-standing ethnic divide between **Meiteis** (Hindu, valley) and **hill tribes (Kukis & Nagas)**; colonial demarcations and post-independence land tensions.
2. Ethnic Composition	Meiteis (~60% of population, political dominance); Kukis & Zomis (hill tribes seeking autonomy); Nagas spread across Nagaland & Manipur.
3. Trigger (2023)	**Meitei demand for Scheduled Tribe (ST) status**; *Manipur HC's April 2023 order* expedited ST recommendations—sparked clashes.
4. Underlying Reasons	ST demand vs land encroachment allegations, religious divisions, and **Myanmar refugee influx** intensified instability.
5. Governance Issues	**Political instability, weak conflict resolution, and delayed delimitation** (first since 1973).
6. Escalation of Violence	**Army & CAPFs deployment failed** to curb clashes; **Internally Displaced Persons (IDPs)** crisis worsened.
7. Root Socio-Economic Causes	**Tribal underdevelopment, poor infrastructure, and unemployment**; Meiteis seek ST to gain affirmative benefits.
8. Key Flashpoints	• *Eviction drives* in protected forests. • *Drug trafficking crackdown* created resentment. • *Kuki Infiltration & Refugee fears.*
9. Steps for Normalisation	**Ensure impartial law enforcement**, facilitate **inclusive dialogue**, promote **ethnic harmony**, and rebuild trust through development.

E. Tripura

Aspect	Details
1. Insurgency	Militancy by **NLFT** and **ATTF** has subsided since 1990s, with peace restored through accords and development.
2. Causes	**Tribal displacement** due to Bengali migration; unemployment and poverty fueled militancy.
3. Measures Taken	**Tripura Peace Accord (1993)** addressed tribal aspirations; **PM GatiShakti** enhanced connectivity and infrastructure.

F. Meghalaya

Aspect	Details
1. Insurgency	Low-intensity militancy by **GNLA** and **HNLC**; extortion and localised violence persist.
2. Causes	**Tribal unemployment** and weak governance; **ethnic tensions with settlers** drive unrest.
3. Measures Taken	**CAPF's Civic Action Programme** and **ROSHNI's skill initiatives** empower youth; **Assam Rifles** ensures border stability.

G. Arunachal Pradesh

Aspect	Details
1. Insurgency	Minimal militancy, but **spillover from NSCN (Nagaland)** and **ULFA (Assam)** poses challenges.
2. Causes	**Proximity to Indo–Myanmar border**, underdevelopment, and **border disputes with China.**
3. Measures Taken	**BRO strengthens infrastructure**, **PM-DevINE** supports growth, **ITBP** manages border.

H. Mizoram

Aspect	Details
1. Insurgency	Peaceful since **Mizo Accord (1986)**; minor militancy by **HPC-D**.
2. Causes	Historical grievances from **1966 famine** and ethnic divides; spillover from Manipur instability.
3. Measures Taken	**Aspirational Blocks Programme** and **community policing** sustain peace and trust.

I. Sikkim

Aspect	Details
1. Insurgency	**Insurgency-free**, with no active groups; stable governance and ethnic harmony.
2. Causes	Minimal ethnic tensions; **tourism-driven growth** ensures stability.
3. Measures Taken	**Proactive policing**, **community engagement**, and **PM GatiShakti** boost cohesion.

3. Impacts of North-East Insurgency

Impact	Description	Examples
1. Human Cost	Thousands killed, **internal displacement**, humanitarian crises.	*250+ deaths and 70,000 displaced* in Manipur (2023).
2. Economic Loss	Projects stalled, trade disrupted, **counter-insurgency costs strain budgets.**	*66 MW Loktak Project* delayed; completion by 2027.
3. Social Disruption	**Ethnic clashes** and **forced migrations** alter demography.	*Bodo-Assamese riots (2012)* displaced 4 lakh.
4. Political Instability	**Insurgent campaigns** undermine governance.	*ULFA anti-election violence (1990s).*
5. Security Challenges	**Drug trafficking, arms smuggling**, and **strain on CAPFs**.	*243 violent incidents (2023); 187 in Manipur.*

4. Initiatives for North-East

Initiative	Description	Examples
1. Peace Accords	Negotiated settlements granting autonomy and mainstreaming insurgents.	*Assam Accord (1985)*, *Naga Accord (2015)*, *Bodo Accord (2020).*
2. Development Schemes	Targeted infrastructure & employment programs.	*PM GatiShakti, PM DevINE.*
3. Legislative Measures	**Sixth Schedule Areas** provide autonomy to tribal councils.	*Assam, Meghalaya, Tripura, Mizoram.*
4. Fiscal Measures	**DoNER Ministry & PM DevINE** for balanced regional growth.	*North-East Business Summit.*
5. Security Measures	**CAPF & special units** neutralise militant activities.	*Operation All Clear, Black Panther Battalion.*
6. Connectivity Projects	Roads, rail, and internet integration.	*BRO highways, LWE Mobile Tower in Tripura.*
7. Border Management Reform	**Scrapping Free Movement Regime (FMR)**; fencing Indo–Myanmar border.	*1,643-km border fencing plan (2024).*
8. Skill Development	**Youth training & employment** to reduce recruitment.	*Skill India Mission, NE Apprenticeship Pilot Scheme.*
9. Civic Action	**Community engagement** by CAPF to counter propaganda.	*CRPF & Assam Rifles programs.*
10. International Cooperation	**Bilateral pacts** to curb cross-border insurgency.	*India–Myanmar cooperation; NSCN camp targeting.*

5. Way Forward for Insurgency in North-East India

Recommendation	Description
1. Legal Reforms & Human Rights	Repeal **AFSPA**, ensure accountability (Jeevan Reddy Committee, 2004); uphold **Naga People's Movement (1997)** demand for grievance redressal.
2. Inclusive Political Dialogue	Revive peace talks with civil society; draw lessons from *Mizoram Accord (1986)* and *Naga Peace Talks.*
3. Decentralized Governance	Strengthen **Autonomous District Councils (ADCs)** for participatory governance (2nd ARC, Tripura ADC 1988).
4. Socio-Economic Integration	Accelerate **PM DevINE**, **Act East Policy**, and **AIIMS Guwahati** for inclusive development and job creation.
5. Regional & Cross-Border Cooperation	Strengthen intelligence-sharing with Myanmar/Bangladesh; expand *India–Myanmar–Thailand Highway.*
6. Community-Centric Counterinsurgency	Prioritise **minimum force, cultural sensitivity**, and **clear-hold-build** strategies.
7. Civil Society & Youth Engagement	Empower women/youth via *Skill India, Khelo India,* and promote cultural integration (e.g., *Hornbill Festival*).

Insurgency in North-East India has declined due to peace accords and development, but persistent **ethnic, political, and economic challenges** require sustained attention.
Long-term peace demands **inclusive governance, border security, and cultural sensitivity**, guided by the **EAST framework — Empower, Act, Strengthen, Transform.**

3.2 Role of external, State and non-State actors in creating challenges to internal security; Challenges to internal security through communication networks; role of media and social networking sites in internal security challenges

Challenges to Internal Security Emerging from External State Actors

India shares over **15,000 km of borders with seven countries**, including **Pakistan, China, and Bangladesh**, many of which are porous or disputed.
This **extensive boundary exposes India** to internal security challenges from external state actors who support **terrorism, insurgency, and cross-border infiltration** to destabilise the nation.

Challenges	Explanation	Example
1. State-Sponsored Terrorism	External states provide funding, training, and safe havens to terrorist groups, undermining national security.	In April 2025, the *Resistance Front (TRF)* claimed the **Pahalgam terror attack**, later designated by the U.S. as a Lashkar proxy.
2. Proxy Warfare & Hybrid Tactics	Use of non-state actors, cyberattacks, and disinformation campaigns to destabilise India strategically.	*Indian Army's drone strike on ULFA's Myanmar headquarters (2025)* has disrupted China and Pakistan's alleged role in reigniting insurgency in Northeast India.
3. Cross-Border Insurgency Support	Neighbouring countries offer safe havens, training, and logistics to insurgent groups in Northeast India.	*China provided moral and material support to Naga insurgents* during the 1960s and 1970s.

4. Cybersecurity Threats	Foreign intelligence agencies conduct cyber espionage and attacks on **critical infrastructure**.	*APT41*, a **Chinese state-sponsored Advanced Persistent Threat group**, targeted India's critical infrastructure.
5. Arms & Drug Smuggling	Narcotics and arms smuggling fund terrorism and insurgency, aiding militant networks and destabilising security in vulnerable border regions.	*"Udta Rajasthan" phenomenon:* By mid-2024–25, Rajasthan became India's main drug entry point from Pakistan, with drone-based heroin drops across Rajasthan's desert border.
6. Radicalisation via Digital Media	External actors exploit social media to spread extremist ideologies and incite communal violence.	*The National Investigation Agency (NIA)* arrested **two women in Kannur in 2021** for alleged ISIS links.
7. Maritime Security Threats	Coastal routes are exploited for arms, drugs smuggling and radical infiltration by hostile actors.	*Gujarat Anti-Terrorist Squad and Indian Coast Guard* seized **over 300 kg of methamphetamine worth ₹1,800 crore**, dumped into the Arabian Sea by Pakistan.
8. Economic Subversion	Dumping counterfeit currency and using hawala networks to destabilise the economy.	*RBI's 2024–25 report* shows a **37% rise in fake ₹500 notes in circulation**, signifying renewed penetration of high-quality counterfeit currency linked to terror-finance routes.
9. Diplomatic Shielding of Terror	Some external actors protect terrorist groups diplomatically, blocking international sanctions.	*FATF's 2025 statement introduced "state sponsorship" of terrorism* and accused India's stance against Pakistan for supporting UN-proscribed terror groups like LeT and JeM.

State Sponsored Terrorism

State-sponsored terrorism refers to **terrorist acts carried out or supported by a government** through funding, training, shelter, or logistical aid to non-state terrorist groups to achieve **its political or strategic objectives**.
It involves a state enabling, otherwise autonomous, terrorist organisations to conduct violence against its adversaries, often covertly.

Ways	Explanation	Example
1. Safe Haven for Terrorist Groups	States provide sanctuary and protection to terrorist groups within their territory, allowing them to plan and launch attacks.	*Pakistan is hosting Lashkar-e-Taiba and Jaish-e-Mohammed*, who carry out attacks in India and find refuge in Pakistan.
2. Training and Recruitment	States establish or allow training camps where terrorists are	*Pakistan's Inter-Services Intelligence* trains militants for

	indoctrinated and trained in **guerrilla warfare and bomb-making**.	operations in Kashmir and Afghanistan.
3. Financial and Logistical Support	States supply funds, weapons, ammunition, and intelligence to terrorist groups to sustain their operations.	*Pakistan is reported to spend around $5 million annually to support militancy in Kashmir.*
4. Facilitation of Terrorist Infiltration	States assist terrorists in crossing borders through **safe passage, forged documents, and logistical help** to conduct attacks.	*Infiltration of militants from Pakistan into Indian-administered Kashmir.*
5. State-Sponsored Radicalization	States promote extremist ideologies and radicalise populations to support terrorism.	*Iran supports Shiite militant groups like Hezbollah in Lebanon and Syria.*

2. Refugee Crisis

Aspect	Explanation	Example
1. Definition	Refugees are individuals forced to flee their home countries due to war, persecution, or violence. Unregulated refugee inflows pose humanitarian and security challenges.	*Rohingya Muslims* fleeing Myanmar settled in parts of India such as Jammu, Hyderabad, and Delhi.
2. Security Implications	Potential for infiltration of **anti-national elements, radicalisation, communal conflict, and demographic imbalance** in sensitive border regions.	*Intelligence agencies flagged suspected links between radical groups and Rohingya settlements.*
3. Strain on Resources & Governance	A sudden influx can burden urban services, public housing, and welfare systems, leading to resentment among local populations.	*In Assam, influx of undocumented migrants* has strained administrative systems and social harmony.
4. Legal and Policy Vacuum	*India lacks a specific domestic law* on refugees and is not a signatory to the 1951 UN Refugee Convention, leading to inconsistent refugee treatment.	*Differentiated treatment of Tibetan refugees, Sri Lankan Tamils, and Rohingya Muslims.*

3. Measures to Tackle Challenges from External State Actors

Measures	Description	Example
1. Strengthen Border Management	Enhance surveillance, deploy more border forces, and use advanced technology (thermal	*India has bolstered Indo-Bangladesh border security* through enhanced manpower, surveillance tech like Hand Held Thermal Imager (HHTI), Night Vision Device (NVD), UAVs, CCTV/

	sensors) to prevent infiltration.	PTZ cameras, IR sensors, and the Comprehensive Integrated Border Management System (CIBMS).*
2. Boost Intelligence and Security Coordination	Improve intelligence sharing among security agencies and enhance cybersecurity capabilities.	*Revamped Multi-Agency Centre (MAC)* now uses AI/ML and real-time satellite imagery to enhance intelligence processing for better threat response.
3. Enhance Diplomatic Engagement	Use diplomatic channels to address cross-border terrorism and seek international cooperation against state-sponsored threats.	*At the 2025 SCO Summit, India called for a united stand against cross-border terrorism*, indirectly highlighting Pakistan's support for terror groups.
4. Modernise Defence and Security Infrastructure	Upgrade military capabilities, secure critical infrastructure, and strengthen counter-terrorism forces.	*India operationalised the S-400 Triumf system in Rajasthan* to counter aerial threats amid heightened tensions post the 2024 Uri-like infiltration attempt.
5. Promote Development in Affected Regions	Implement development schemes to reduce alienation and insurgency recruitment.	Under *Vibrant Villages Programme and Border Area Development Programme*, India is developing remote border villages to deter Chinese influence and address the needs of border populations.

Challenges to internal security from external state actors, including terrorism, proxy warfare, and cyber threats, undermine India's stability and sovereignty. As S. Jaishankar aptly noted, "If activities across borders are characterised by terrorism, extremism, and separatism, they are hardly likely to encourage trade, energy flows, connectivity and people-to-people exchanges in parallel."
This highlights the urgent need for a **comprehensive and coordinated security response.**

Challenges to internal security emerging from non-state actors

Non-state actors such as *insurgent groups, terrorist organisations, and transnational criminal networks* pose complex and evolving threats to India's internal security.
Their activities **undermine national stability** by exploiting technological tools, porous borders, and socio-political vulnerabilities.

UPSC Previous Year Question

1. 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. **(2023)**
2. Discuss the types of organised crime. Describe the linkages between terrorists and organised crime that exist at the national and transnational levels. **(2022)**
3. 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 these threats. **(2021)**
4. Use of the internet and social media by non-state actors for subversive activities is a major security concern. How have these been misused in the recent past? Suggest effective guidelines to curb the above threat. **(2016)**

---

1. Factors enabling the rise of Non-State Actors

Aspect	Explanation
1. Asymmetrical Warfare	Non-state actors employ unconventional and unpredictable tactics that challenge traditional security responses.
2. Cross-border Support	Non-state actors receive funding, training, or sanctuary from hostile states like Pakistan's ISI, enabling groups like LeT to sustain operations.
3. Weak Governance in Conflict Zones	These groups exploit local grievances and governance vacuums in underdeveloped or conflict-affected regions.
4. Technology Use	They utilise advanced technologies like encrypted communications, cryptocurrencies, and drones to enhance their capabilities.
5. Social Polarization	Non-state actors manipulate caste, religious, and ethnic divisions to recruit members and incite violence.

---

2. Challenges to internal security emerging from non-state actors

Challenge	Description	Example
1. Terrorism	Non-state terrorist groups use suicide bombings, drone attacks, and IEDs to instil fear, disrupt governance, and challenge state authority.	*Dangri terror attack in Rajouri, J&K (2023)*, killed seven civilians through gunfire and grenade assault, followed by an IED explosion the next day.
2. Left-Wing Extremism (LWE)	Armed Maoist groups, operating in tribal regions and mineral-rich areas, engage in anti-state rebellion.	*In 2025, in a major anti-Naxal operation at Kangerghati Hills (Chhattisgarh-Telangana border)*, security forces neutralised 31 Maoists, marking a significant blow to LWE.

3. Cyber Threats	Hackers targeting digital infrastructure for espionage, misinformation, and financial crimes.	*APT41*, a Chinese state-sponsored Advanced Persistent Threat (APT) group, targeted India's critical infrastructure including *Air India (2021)*.
4. Organized Crime	Drug trafficking, human trafficking, and arms smuggling that undermine governance and fuel instability.	*In 2025, BSF recovered 100 Pakistani drones along the Punjab border (294 drones in 2024)*, linked to Pak-based terror groups—seizing heroin, arms, and explosives.
5. Religious/Communal Extremism	Radical groups are spreading hatred, provoking communal violence, and recruiting vulnerable individuals.	*In 2023, PFI (banned in 2022)* operatives were arrested in Kerala for inciting communal violence.
6. Insurgency Movements	Ethnic or separatist groups control conflict-prone border areas, challenging state sovereignty.	*The Meitei-Kuki conflict in Manipur*, triggered by ST status demands, led to ethnic violence and looting of more than 6,000 weapons.
7. Foreign-funded NGOs (alleged)	Some NGOs allegedly misuse foreign funds to fuel dissent and protest infrastructure projects.	*FCRA cancellation of Greenpeace and Amnesty International India.*
8. Information Warfare & Fake News	Disinformation spread via social media incites violence and manipulates public opinion.	*Manipur violence 2023: Fake videos circulated via WhatsApp and Facebook* worsened ethnic tensions, spreading panic and fueling retaliatory attacks.
9. Urban Naxalism	Intellectual and ideological support to Maoists through academia or civil society organisations.	*Elgar Parishad–Bhima Koregaon case (2018).*
10. Youth Radicalization	Use of the internet and social media to ideologically radicalise youth towards extremist causes.	*In 2017, a Hyderabad youth was arrested for alleged involvement in an ISIS module.*

3. Hooda Committee (2019) Recommendations

Aspect	Recommendation
1. Neighbourhood Relations	Strengthen regional ties by leveraging soft power, enhancing connectivity, and promoting trade with neighbouring countries.
2. Internal Conflicts	Resolve conflicts in *Jammu & Kashmir*, the *Northeast*, and *Left-Wing Extremism-affected areas* through development, integration, and counter-radicalisation efforts.

3. Citizen Protection	Prioritise protecting citizens from cyber threats, terrorism, and insurgencies through proactive security measures.
4. Capability Enhancement	Enhance India's ability to protect its citizens and deter adversaries by securing both land and maritime borders effectively.

4. Measures proposed in the Budget (2025–26) to Strengthen Internal Security

Aspect	Recommendation
1. Jammu & Kashmir Security	Eliminate terror networks, prevent infiltration, and dismantle terror financing to make Jammu & Kashmir terror-free.
2. North East Insurgency	Integrate insurgent groups into the peace process and strengthen border security to curb infiltration in the Northeast.
3. Left-Wing Extremism	Eradicate Left-Wing Extremism through focused security and development measures.
4. Criminal Justice Modernisation	Modernise the criminal justice system by digitally integrating police, judiciary, forensics, prisons, and prosecution for better crime prevention and justice delivery.
5. Police & CAPF Modernisation	Upgrade police and Central Armed Police Forces (CAPF) with advanced equipment, automation, interoperability, and welfare initiatives.
6. Cybercrime Infrastructure	Strengthen cybercrime response through the *Indian Cyber Crime Coordination Centre (I4C)*, cyber fraud centres, suspect registry, and national cyber threat intelligence.
7. Border & Coastal Security	Enhance border and coastal security with technological upgrades like drones, surveillance, fencing, digitised mapping, and improved coordination among security agencies.
8. Narcotics Control & Disaster Preparedness	Enforce zero tolerance against narcotics and improve disaster preparedness through community participation, better-equipped response forces, and international cooperation.
9. Immigration System Modernisation	Streamline visa issuance, promote e-visas, and fast-track clearance for trusted travellers at major international airports.

5. Way Forward

Aspect	Description
1. Strengthen Intelligence	Enhance coordination among the *Multi-Agency Centre (MAC)*, State Police, NIA, and other agencies for timely intelligence sharing, as recommended by the *Kargil Review Committee (1999)* to overhaul India's intelligence and internal security system.
2. 'Whole of Government' Approach	Based on coordination among all wings and the concept of *Team India* to enable effective response to internal security challenges while building a self-reliant and strong nation.
3. Cyber Security Architecture	Implement the *National Cyber Security Strategy* to build a robust framework protecting critical infrastructure and counter cyber threats.

4. Counter-Radicalization Measures	Promote community policing and de-radicalisation initiatives like *Kerala's model*, which emphasises strong police-public partnerships and proactive community engagement to prevent extremist recruitment and maintain social harmony.
5. Border Management	Deploy technology-driven solutions, including smart fencing, *Integrated Check Posts (ICPs)*, and drone surveillance for effective border security.
6. Financial Tracking	Strengthen the *Financial Intelligence Unit – India (FIU-IND)* and enhance enforcement of laws under the *Prevention of Money Laundering Act (PMLA)* and the *Unlawful Activities (Prevention) Act (UAPA).*
7. Engagement with Civil Society	Encourage credible NGOs to actively participate in peacebuilding and development efforts in conflict-affected areas.

Effectively countering threats from non-state actors requires a comprehensive strategy involving **robust intelligence, seamless inter-agency collaboration, active community participation, and technology-enabled policing**, complemented by **de-radicalisation efforts and strengthened border security**.
As Rajnath Singh highlighted, *"India's security apparatus must remain adaptive to emerging threats such as cyber warfare, hybrid warfare, space-based challenges, and transnational organised crime."*

Challenges to internal security through communication networks

India's increasing **dependence on communication networks** such as the *internet and mobile phones* has introduced significant **internal security challenges**.
Extremist and criminal groups exploit these networks for **cyberattacks**, **spreading misinformation**, **radicalization**, and disrupting **critical infrastructure**, thereby threatening **national stability and public order**.

---

1. Challenges through Communication Networks

Challenge	Description
1. Spread of Misinformation and Fake News	Rapid spread of *false information on social media* fuels *communal tensions, panic, and violence.* **Example:** During the *2023–24 Manipur conflict*, fake news on platforms like *WhatsApp and Instagram* exacerbated ethnic violence.
2. Cyberterrorism and Cyber Attacks	*Terrorist and hostile groups* exploit communication networks to attack *critical infrastructure and government systems*,

	threatening national security. **Example:** *Post-Pulwama attack, Pakistan-based APT36 launched cyber-espionage* targeting *Indian defence personnel.*
3. Recruitment and Radicalisation	*Extremist groups use encrypted apps and social media* to recruit and radicalise youth while evading surveillance. **Example:** *APT36 used Android malware like CapraRAT through fake dating apps* to target *military personnel and activists.*
4. Coordination of Anti-National Activities	*Terrorists and insurgents use digital platforms* to plan attacks and share intelligence, complicating counter-terror efforts. **Example:** A new app, *"Calculator,"* found on the smartphones of terrorists in *Jammu and Kashmir,* helps them remain in touch with their handlers in *Pakistan-occupied Kashmir (PoK).*
5. Propagation of Hate Speech and Extremism	*Online platforms are misused* to spread *hate speech and extremist ideologies*, deepening societal divides. **Example:** In *2024, bot-driven hate campaigns* targeting minorities were flagged during the *Lok Sabha pre-election period.*
6. Fake Accounts and Bot Networks	The use of *fake profiles and bots* manipulates *public opinion* and destabilises *social harmony.* **Example:** A recent report by *Meta* highlighted the growing *menace of fake Facebook accounts* originating from *China,* spreading *fake news about India.*
7. Technical Challenges in Monitoring	*Encrypted messaging apps and VPNs* hinder *real-time monitoring and interception* by security agencies. **Example:** *Encrypted Telegram channels* were used by *IS sympathisers in South India* to bypass surveillance in 2025.

2. Measures Needed to Strengthen Communication Network

Aspect	Recommendation
1. Strengthen Cybersecurity Framework	Implement robust cybersecurity policies like the *National Cyber Security Strategy* to protect *critical infrastructure and data.*
2. Enhance Incident Response & Coordination	Empower agencies such as *CERT-In* and *Indian Cyber Crime Coordination Centre (I4C)* for rapid detection and coordinated response to cyber threats.
3. Capacity Building & Awareness	Promote *digital literacy* and *cyber hygiene* through campaigns like *Cyber Swachhta Kendra* and *NCERT's cyber safety modules* to reduce vulnerabilities to misinformation and cyberattacks.
4. Legal and Regulatory Strengthening	Update and enforce laws to effectively tackle *cybercrime* and *regulate social media* to curb misinformation while balancing *privacy concerns.*

5. Inter-Agency and International Cooperation	Foster collaboration among *NCIIPC*, *I4C*, and *global partners* under frameworks like the *Budapest Convention* to combat *cross-border cyber threats* and terrorism.

India's communication networks face security threats like cyberattacks, misinformation, and radicalisation.
Addressing these requires **robust cybersecurity policies, updated legal frameworks, public awareness campaigns, and coordinated efforts**.
Balancing **surveillance needs with privacy rights** is crucial for national security and stability.

Role of media and social networking sites in internal security challenges

Media and social media are pivotal in shaping internal security dynamics, influencing public perception, and facilitating rapid crisis response.
As **Edward Tufte** insightfully noted, *"There are only two industries that call their customers 'users': illegal drugs and software,"* highlighting the addictive and manipulative potential of social media platforms.

These tools amplify awareness, aid intelligence gathering, and counter misinformation but also pose **risks through fake news and radicalization**, necessitating vigilant monitoring and strategic communication to safeguard national stability.

UPSC Previous Year Question

1. 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. **(2024)**

---

1. Role of Media in Ensuring Internal Security

Role of Media	Description
1. Watchdog Function	The media hold government and security agencies accountable by **exposing corruption and lapses.** **Example:** In the *2023 Parliament breach*, the media exposed security lapses through footage and debates, triggered public outcry, pressured accountability, and catalysed CISF reforms, reinforcing its watchdog role in internal security.

2. Public Awareness & Education	Educates citizens about threats like **terrorism and cybercrime**, promoting vigilance. **Example:** *Media campaigns on cyber hygiene* and anti-terrorism awareness.
3. Countering Misinformation	**Responsible media counters fake news** and rumours that could incite violence. **Example:** The *PIB Fact Check Unit debunked fake posts* about a "Fidayeen attack" and an alleged strike on Hazira Port during Indo-Pak tensions in May 2025.
4. Promoting National Integration	Highlights unity and condemns divisive forces to foster harmony. **Example:** The *SYS-led 'Soubharda Sanchaar' campaign (2025)* used media-supported interfaith rallies in Coastal Karnataka to counter communal disinformation and hatred.
5. Shaping Public Opinion	Influences support for security policies. **Example:** Media support for **anti-terror laws like UAPA and NIA.**
6. Advocacy for Policy Reforms	**Investigative journalism and debates** push for reforms in security laws and policing. **Example:** Media debates on police reforms post-*Delhi riots 2020* case.
7. Promoting Communal Harmony	Discourages hate speech and reports sensitively on inter-community issues. **Example:** During the *Delhi riots (2020)*, news outlets like *The Hindu* and *NDTV* ran campaigns urging peace and unity, countering divisive narratives.
8. Disaster Management	Media disseminates official advisories and emergency information during crises, spreads timely updates, coordinates relief efforts, and prevents misinformation. **Example:** Media's role in communication and relief efforts during *Kerala Floods.*

2. Threats to Internal Security from the Media

Threats	Description
1. Sensationalism and Misinformation	Sensational reporting spreads panic and misinformation during sensitive situations, worsening security risks. **Example:** *Satara riots (Maharashtra): Viral Instagram posts instigating Hindu deities sparked communal violence.*
2. Live Coverage of Security Operations	Real-time telecasts can reveal tactical details, **compromising security forces and aiding adversaries.** **Example:** Live coverage during the *26/11 Mumbai attacks* helped terrorists track security forces' movements.
3. Communal Polarization	**Biased or irresponsible reporting** can inflame communal tensions and provoke violence. **Example:** *A 2022 report criticised major Indian TV news*

	channels for promoting anti-Muslim prejudice and sensationalising the *2020 Delhi riots.*
4. Propagation of Fake News	Fake news and rumours in the media and on social platforms can **trigger mob violence and public disorder.** **Example:** *Mangaluru lynching case:* Police filed FIRs against social media users for spreading false and inflammatory WhatsApp posts falsely claiming a lynching occurred.
5. Leakage of Classified Information	**Unauthorised disclosures** can endanger **national security** and diplomatic relations. **Example:** *Media leaks on sensitive defence matters* can compromise operations.
6. Trial by Media	Media trials can prejudice investigations and judicial processes, affecting fairness and rights. **Example:** *Media trial in the Sushant Singh Rajput case* influenced public opinion and judicial proceedings.
7. Compromising Victim Dignity	**Irresponsible reporting** may expose victims' identities and sensitive details, risking safety and dignity. **Example:** *Media exposure of rape victims' identities* violates privacy and safety norms.

3. Role of Social Media in Ensuring Internal Security

Social media refers to online platforms where users share information and connect with virtual communities through text, video, photos, and other content. In January 2025, India had 491 million social media user identities, which accounted for **33.7% of the population.**

Role	Description
1. Early Warning and Rapid Information Dissemination	Social media enables authorities to **quickly share alerts and advisories** during emergencies (disaster warnings, terror threats), enhancing public preparedness. **Example:** *Odisha Police X handle (2024)* actively updated citizens during *Cyclone Michang,* sharing evacuation and safety advisories.
2. Crowdsourcing Intelligence	Citizens can report suspicious activities or incidents in real time, aiding law enforcement. **Example:** *Delhi Police's WhatsApp helpline* for reporting crimes and rumours.
3. Countering Misinformation and Rumors	Governments and agencies use official accounts to **debunk fake news** and clarify facts, preventing panic and unrest. **Example:** *PIB Fact Check on Twitter* during COVID-19.
4. Promoting Community Policing	Police and security agencies engage with citizens, **building trust and encouraging cooperation** in maintaining law and order. **Example:** *Mumbai Police's active presence* on social media for public outreach.

5. Facilitating Disaster Management	Social media platforms are used for coordinating rescue and relief operations, **mobilising volunteers**, and providing real-time updates. **Example:** *Use of local Twitter handles during Kerala floods* for rescue coordination.
6. Monitoring and Preventing Extremism	Security agencies **monitor social media for radicalisation, hate speech, and terror propaganda**, allowing timely interception. **Example:** *Tracking ISIS-related activities and online radicalisation cases.*
7. Public Awareness and Education	Social media is used to **spread awareness about cybersecurity, anti-terrorism, and responsible citizenship.** **Example:** *#CyberSafeIndia campaign* by government agencies.

4. Threats to Internal Security from Social Media

Threats	Description
1. Radicalization and Recruitment	Terror groups like **ISIS, AQIS, and LeT use social media platforms** (Telegram, Twitter, YouTube) to spread propaganda and recruit youth. NIA has intercepted such networks.
2. Misinformation and Fake News	Rapid spread of false information fuels communal tensions and mob violence. **Example:** *Child-lifting rumours on WhatsApp* led to lynchings in Maharashtra.
3. Communal Polarization and Hate Speech	Social media amplifies **divisive narratives and hate speech**, worsening communal relations. **Example:** *Role in exacerbating 2020 Delhi riots.*
4. Cyber Terrorism and Crime	Platforms are exploited for planning terror attacks, cyber fraud, hacking, and spreading extremist content. **Example:** *Use of encrypted apps for terror coordination.*
5. Foreign Interference and Propaganda	Foreign actors use social media to **influence public opinion, spread fake news, and disrupt political stability.** **Example:** *Alleged foreign funding of divisive campaigns.*
6. Privacy Breaches and Surveillance Issues	**Personal data misuse** and digital surveillance raise concerns over privacy violations and potential misuse of information.
7. Real-time Coordination of Protests and Riots	Social media facilitates **rapid mobilization of protests**, which can escalate into violence and law and order problems.
8. Anonymity and Encrypted Communication	Use of encrypted messaging apps **hinders monitoring of extremist activities**, complicating counter-terrorism efforts.

9. Challenges in Regulation and Enforcement	Jurisdictional issues, data localisation, and balancing freedom of expression with security complicate effective regulation.

5. Existing Measures and Legislation

Measure	Description
1. Article 19(1)(a) of the Constitution	Guarantees freedom of speech and expression, subject to **reasonable restrictions** in the interest of *sovereignty, security,* etc.
2. Press Council Act, 1978	Establishes the Press Council of India to **preserve press freedom and maintain ethical standards** in journalism.
3. National Security Act, 1980	Allows the government to impose **restrictions on press** reporting if it threatens national security.
4. Broadcasting Code (All India Radio, TV)	Sets standards for **objective, fair, and unbiased broadcasting; prohibits content threatening national security.**
5. News Broadcasting Standards Authority (NBSA)	A **self-regulatory body enforcing ethical standards** for TV news channels.
6. Information Technology Act, 2000 & Related Provisions	Regulates electronic communication; includes **Section 69A (content blocking for security)**, **Section 79 (safe harbour for intermediaries).**
7. Section 69A of IT Act	**Empowers government to block public access** to information threatening sovereignty, security, or public order.
8. Section 79 of IT Act	Provides **safe harbour to intermediaries** (social media platforms), conditional on due diligence and content removal.
9. IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021	**Mandates social media platforms** to follow due diligence, appoint compliance officers, and implement grievance redressal mechanisms.
10. CERT-In (Indian Computer Emergency Response Team)	**Issues cybersecurity guidelines and advisories** to prevent misuse of social media and cyber threats.
11. Digital Personal Data Protection Act, 2023	**Regulates personal data handling** by digital platforms to protect user privacy and prevent data misuse, enhancing social media security.

6. Way Forward

Suggestions	Description
1. Promote Responsible Journalism	Encourage **fact-checking**, editorial accountability, and avoid sensationalism to prevent misinformation and panic.

2. Strengthen Regulation of Sensitive Information	Enforce laws to prevent **unauthorised disclosure** of classified or sensitive information.
3. Enhance Media Training and Strategic Awareness	Train journalists and media personnel on **national security issues** to ensure informed and mature coverage.
4. Regulate Live Coverage of Security Operations	Impose guidelines to **restrict live telecast** of sensitive anti-terror or security operations to protect operational secrecy.
5. Monitor and Counter Misinformation on Social Media	Use **AI tools, fact-checking**, and collaboration between government and platforms to curb fake news and hate speech.
6. Integrate Media in Crisis Communication	Utilize media for **timely dissemination of accurate information** during crises to aid public coordination.
7. Promote Digital Literacy and Public Awareness	Educate citizens on **responsible media consumption** and recognising misinformation to reduce social unrest.
8. Foster Collaboration Between Media, Security Agencies, and Government	Establish regular dialogue and **protocols for verified information sharing** to build trust and effective communication.
9. Ensure Equitable Enforcement of Media Laws	Apply laws fairly to prevent arbitrary penalties and **avoid media trials** that destabilise internal security.

Media and social media play a pivotal role in shaping internal security dynamics. While they facilitate rapid information dissemination and crisis management, their misuse can amplify misinformation, hate speech, and unrest.
As **Sundar Pichai**, CEO of Google, emphasised during the Google for India event,
"Technology needs responsible regulation as it touches so many lives."
This underscores the necessity for **balanced frameworks** that safeguard citizens while fostering innovation. Ensuring the **responsible use of digital platforms** is essential to maintain national security and social harmony.

3.3 Basics of cyber security; money-laundering and its prevention

Cybersecurity

Cybersecurity, as defined by India's *National Cyber Security Policy (2013)*, refers to the protection of information, devices, services, and systems in cyberspace from unauthorised access, attacks, damage, or disruption.

With **India's digital landscape** expanding rapidly, boasting **936 million internet subscribers** (TRAI, Dec 2023), and platforms like **Aadhaar, UPI, and Digital India** driving

transformation, cybersecurity is a national imperative. The **country reported 20.41 lakh cybercrime incidents** in 2024 (as per CERT-In), ranging from ransomware and phishing to misinformation and critical infrastructure attacks.

With growing reliance on digital governance, financial technologies, and data-centric services, ensuring a **secure cyber ecosystem** is crucial for safeguarding national security, economic stability, and individual privacy.

UPSC Previous Year Question

1. What are the different elements of cybersecurity? Keeping in view the challenges in cybersecurity, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**
2. Keeping in view India's internal security, analyse the impact of cross-border cyber-attacks. Also, discuss defensive measures against these sophisticated attacks. **(2021)**
3. Discuss different types of Cyber crimes and measures required to be taken to fight the menace. **(2020)**
4. Data security has assumed significant importance in the digitised 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? **(2018)**
5. Discuss the potential threats of Cyber attacks and the security framework to prevent it. **(2017)**
6. Considering the threats cyberspace poses for the country, India needs a "Digital Armed Forces" to prevent crimes. Critically evaluate the *National Cyber Security Policy, 2013*, outlining the challenges perceived in its effective implementation. **(2015)**
7. Cyber warfare is considered by some defence analysts to be a larger threat than even Al Qaeda or terrorism. What do you understand by Cyber warfare? Outline the cyber threats to which India is vulnerable and bring out the state of the country's preparedness to deal with the same. **(2013)**

---

1. Types of Cyberthreats

Threat Type	Description	Example
1. Malware	Malicious software (like *ransomware, spyware, trojans*) is used to damage systems, steal data, or gain unauthorised access.	*WannaCry Ransomware (2017):* Hit several Indian systems, including hospitals and banks.
2. Denial-of-Service (DoS)	Flood networks or servers with excessive traffic to crash or disable services; DDoS uses multiple systems for greater impact.	*DoS attack on AIIMS Delhi (2022):* Patient care and servers crippled for days.

3. Phishing	Deceptive emails, SMS, or fake websites that impersonate trusted sources to steal login credentials, OTPs, or personal data.	*COVID-19 Vaccine Registration Scam (2021):* Fake CoWIN links led to data theft.
4. Spoofing	Forging email headers, IP addresses, or websites to appear legitimate and trick users or systems into trusting the attacker.	*CERT-In alert (2022):* Rise in spoofed govt. domain emails (e.g., @gov.in) targeting officials.
5. Identity-Based Attacks	Using stolen or fabricated identities and login credentials to commit fraud, impersonate users, or bypass security.	*Aadhaar Data Leak (2018):* Unauthorised access to Aadhaar holders' data.
6. Code Injection Attacks	Inserting harmful code (such as SQL injection, XSS) into applications to exploit flaws, steal data, or hijack functionality.	*BHIM-UPI phishing via malicious code* embedded in apps.
7. Supply Chain Attacks	Infiltrating through third-party vendors, software updates, or hardware components to compromise larger target networks.	*2021 Upstox Data Breach:* Hacker accessed sensitive KYC info via third-party cloud misconfiguration.
8. Social Engineering	Psychological manipulation of individuals to reveal confidential information or grant system access (e.g., posing as IT staff).	*WhatsApp OTP frauds (2021-23):* Many lost UPI access due to manipulative calls from fake agents.
9. Insider Threats	Employees or insiders misusing authorised access for theft, sabotage, or data leaks, intentionally or accidentally.	*Air India (2021):* Data breach included internal access misuse, exposing 4.5 million fliers.
10. DNS Tunneling	Abuses DNS protocol to covertly transmit stolen data or maintain communication with compromised systems.	*Suspected usage in cross-border spying attempts.*
11. IoT-Based Attacks	Exploiting security flaws in connected devices like CCTVs, routers, or smart appliances for control or spying.	*Indian smart cameras and routers compromised* during Chinese botnet campaigns.
12. AI-Powered Attacks	Leveraging AI/ML to launch sophisticated attacks like *deepfakes, automated phishing, or adaptive malware* that evades detection.	*2024 Elections:* Deepfake videos of politicians circulated on WhatsApp and Instagram Reels.

2. Need for Cybersecurity in India

Reason	Description	Substantiation
1. Anonymity & Detection Challenges	Cyberattacks are hard to detect, investigate, and attribute due to anonymity and global digital infrastructure.	*Only 18% of cybercrime cases in India* resulted in *successful conviction (NCRB, 2024).*
2. Evolving & Innovative Threats	Cybercriminals use *new, inventive techniques*, making traditional defences less effective.	Surge in attacks using *Ransomware-as-a-Service (RaaS)* and *Cybercrime-as-a-Service (LockBit, Akira).*
3. Misuse of Artificial Intelligence	AI tools (such as *WormGPT*) are exploited to *automate phishing, generate malware, and spread disinformation.*	*WormGPT* is used to craft phishing emails and malware, detected in *Indian BFSI sector attacks.*
4. Terrorism & National Security	Terror groups use *DDoS, malware, and phishing* to disrupt services and spread propaganda.	*2024: CERT-In flagged DDoS attacks* targeting Indian defence and communications networks.
5. Digitisation & Financial Risks	*Rapid digitisation* (UPI, Aadhaar, e-Governance) increases exposure to fraud, surveillance, and privacy breaches.	*₹33.41 crore saved in 9.94 lakh complaints* via HC's *Citizen Financial Cyber Fraud Reporting System.*
6. Cyber Warfare & State Actors	*State-sponsored cyberattacks* against India have sharply increased, targeting IT, BPO, and government sectors.	*728% rise in state-sponsored attacks* (Cyfirma 2023 India Threat Landscape Report).
7. Rising Cybercrime Incidence	Cybercrime cases are rising rapidly, *outpacing law enforcement and judicial capacity to respond.*	*NCRB: 65,893 cybercrime incidents in 2022* (24.2% rise over 2021).

3. Impacts of Cyber Threats

Impact Area	Description	Example
1. Disruption of Critical Infrastructure	Cyberattacks on *power grids, transport, and health systems* cause service outages, economic loss, and public safety risks.	*Mumbai Power Grid Attack (2020):* Led to city-wide blackout.
2. Large-Scale Data Breaches	Massive leaks of personal, government, or business data threaten privacy, enable identity theft, and erode trust.	*Hi-Tek Group Breach (2024):* 850 million records of Indian citizens leaked, one of the largest breaches globally.
3. Financial Losses & Fraud	Cybercrime in banking and payments results in unauthorised transactions, loss of funds, and undermines digital trust.	*City Union Bank SWIFT Attack (2020):* USD 2 million lost via malware in SWIFT system.

4. National Security Threats	*State-sponsored cyber espionage* targets defence, nuclear, and government networks, risking sovereignty and sensitive data.	*Kudankulam Nuclear Plant Attack (2019):* Malware infiltration attempt; highlighted CII vulnerabilities.
5. Reputational Damage	Breaches and attacks diminish stakeholder trust in institutions, impacting investment, brand value, and digital adoption.	*Airtel Data Breach (2021):* Customer trust shaken after exposure of millions of user records.
6. Economic Impact & Productivity Loss	Cyberattacks cause *direct financial loss*, disrupt business operations, and impede economic growth and competitiveness.	*India ranked 2nd globally in cyber attacks (2024):* 95 major data thefts, 108 ransomware cases in one year.
7. Youth & Social Vulnerability	*Tech-savvy youth* face risks like cyberbullying, online scams, and grooming, increasing societal costs and the digital divide.	*2023: 34% of Indian organisations reported phishing; teenagers* are frequent targets in gaming and social media.

4. Challenges in India's Cybersecurity

Challenge	Description	Example
1. Critical Infrastructure Vulnerability	Cyberattacks targeting *power grids, nuclear plants, and healthcare systems* disrupt essential services, risking public safety and national security.	*AIIMS Attack (2022):* 40 million patient records encrypted; services halted for 14 days. *Kudankulam Nuclear Plant (2019):* Malware (Dtrack) infiltrated systems via phishing.
2. Financial Sector Threats	Cybercriminals exploit banking systems for fraud, causing financial losses and eroding trust in digital transactions.	*2024 Ransomware Attack:* Disrupted payment systems of 300 local banks via a service provider.
3. Data Breaches & Privacy Concerns	Surge in leaks of sensitive personal/government data due to weak safeguards, enabling identity theft and fraud.	*MoChhatua App Breach (2023):* Around 1,500 user details sold on dark web.
4. Cyber Espionage	*State-sponsored hackers* target military, diplomatic, and strategic assets to steal sensitive information.	*Operation SideCopy (2020):* Pakistani group targeted Indian military with malware-laced emails.
5. Advanced Persistent Threats (APTs)	*Sophisticated, long-term cyber intrusions* by foreign actors to sabotage critical systems or steal data.	*RedEcho (2021):* China-linked APT targeted 10 power sector entities with malware to trigger outages.

6. Poor Cyber Hygiene	Lack of *digital literacy* leads to increased vulnerability among rural and senior populations.	Despite training of *over 75,000 police and judicial officers* via *CyTrain platform*, digital illiteracy remains high.
7. Supply Chain Vulnerabilities	Exploitation of third-party software/hardware weaknesses to infiltrate government and corporate networks.	*SolarWinds Attack (2020):* Compromised NIC's systems via infected network tools.

5. Steps Taken by India Towards Cybersecurity

Legal Measures

Measure	Description	Example
1. Information Technology Act, 2000	Defines *cybercrimes* (hacking, cyberterrorism), protects *Critical Information Infrastructure (CII)*, and prescribes penalties.	*BSNL Data Breach (June 2024):* Over 278GB of telecom data exposed, highlighting the Act's role in breach response.
2. Digital Personal Data Protection Act (DPDP), 2023	Balances data processing rights with user privacy, grants rights to access, correct, and erase data.	*DPDP Act Penalty:* Penalties up to ₹250 crore for breaches; draft rules released in April 2025 for phased implementation.
3. National Digital Communications Policy, 2018	Aims for *"Secure India"* through *digital sovereignty, universal broadband, and $100B investments.*	*BharatNet:* 1 Gbps connectivity to 250,000 gram panchayats by 2025.
4. National Cyber Security Policy, 2013	Focuses on CII protection, workforce development, and public-private partnerships.	*Examples:* Targeted *500,000 cybersecurity professionals by 2018;* achieved only 30%.

Institutional Measures

Institution	Role / Description	Example
1. National Critical Information Infrastructure Protection Centre (NCIIPC)	Protects CII under IT Act, Section 70A; monitors sectors like energy and banking.	*Secured 85% of power grids after post-2022 cyberattacks;* designated Aadhaar database as CII.
2. CERT-In	National nodal agency under IT Act, Section 70B; issues alerts and investigates breaches.	*Handled 1.4 million incidents in 2023 (33% YoY rise).*

3. Cyber Swachhta Kendra	*Botnet/malware analysis centre;* provides free tools for device sanitisation.	*E-Kavach:* Installed on 5 million smartphones to block spyware.
4. National Cyber Coordination Centre (NCCC)	Monitors metadata for real-time threat detection; collaborates with ISPs.	—
5. Indian Cyber Crime Coordination Centre (I4C)	MHA-led agency tackling *cyber fraud, child pornography, and darknet crimes.*	*Launched Samvaay Platform* for interstate data sharing.
6. Cyber Fraud Mitigation Centre (CFMC)	Facilitates real-time collaboration among banks, telecoms, and LEAs to tackle financial cyber fraud.	*Citizen Financial Cyber Fraud Reporting and Management System (I4C):* Saved ₹33.41 crore across 9.94 lakh complaints.

6. National Cyber Security Policy 2023

It aims to protect the public and private infrastructure from cyberattacks. The policy also intends to safeguard *"information, such as personal information (of web users), financial and banking information and sovereign data."*

Aspect	Description
1. Objectives	Create a *secure cyber ecosystem*, ensure trust in IT, protect critical infrastructure, and promote global best practices. **Example:** *India achieved Tier-1 status in Global Cybersecurity Index (GCI) 2024* with a 98.49/100 score.
2. Regulatory Framework	Strengthen legal and regulatory mechanisms, mandate audits, and *harmonise with global standards* for cybersecurity. **Example:** *Periodic security audits* are mandated for all government ICT infrastructure.
3. Incident Response Mechanism	Establish *national-level CERT-In* as the nodal agency for cyber emergency response and sectoral CERTs for crisis management. **Example:** *CERT-In issued 1,200+ advisories in 2024* on AI-driven phishing and ransomware.
4. Protection of Critical Information Infrastructure (CII)	Operate *NCIIPC for 24×7 protection*, mandate security audits, and certify security roles for CII operators. **Example:** *NCIIPC secured 85% of power grids* after targeted cyberattacks on the energy sector in 2024.
5. Capacity Building	Target workforce of *500,000 skilled cybersecurity professionals*; promote awareness and skill development in public/private sectors.

	Example: *Only 30% of the target was met by 2023,* hence the skill gap remains a major challenge.
6. International Cooperation	Engage in *global partnerships,* share threat intelligence, and align with international cybersecurity norms and standards. **Example:** *CERT-In signed MoUs with Bangladesh, Egypt, Japan,* and others for cyber threat cooperation.

7. Way Forward for Strengthening India's Cybersecurity

Suggested	Description
1. Strengthen Critical Infrastructure Protection	Prioritise resilience and redundancy in critical infrastructure (power, health, finance) using *Zero Trust Architecture* and regular audits. **Example:** *CERT-In's Cyber Crisis Management Plan (2024)* mandates sector-wise drills; NCIIPC notified as nodal agency under IT Act.
2. Enhance Cyber Workforce and Capacity Building	Scale up cybersecurity skilling through public-private partnerships, integrating AI, blockchain, and forensics in government training. **Example:** *Cyber Surakshit Bharat trained 250+ CISOs in 2024; Cyber Security Grand Challenge 2.0 promotes startup innovation.*
3. Implement Robust Data Protection and Privacy Laws	Enforce *Digital Personal Data Protection Act (DPDP), 2023* with strict breach reporting, data localisation, and user consent frameworks. **Example:** *DPDP Act (2023):* Mandatory 72-hour breach reporting; Aadhaar, health, and fintech sectors under new compliance regime.
4. Foster Public Awareness and Digital Literacy	Launch nationwide awareness campaigns on phishing, social engineering, and safe digital practices, targeting youth, SMEs, and senior citizens. **Example:** *Digital India Initiatives* and *Cyber Jaagrookta Diwas* (monthly awareness day) mandated by MeitY since 2022.
5. Strengthen Legal and Regulatory Ecosystem	Update and harmonise cyber laws (IT Act, DPDP, sectoral guidelines), empower law enforcement with cyber forensics, and rapid reporting tools. **Example:** *Standing Committee on IT (2023)* recommended a unified cyber law.

Money Laundering

Money laundering refers to the *process of disguising the origins of illegally obtained money* to make it appear legitimate. According to the **Financial Action Task Force (FATF)**, money laundering is *"the processing of criminal proceeds to disguise their illegal origin in order to legitimise the ill-gotten gains of crime."*
In India, this crime undermines economic integrity, facilitates corruption, and funds terrorism and organised crime.

UPSC Previous Year Question

1. Discuss how emerging technologies and globalisation contribute to money laundering. Elaborate measures to tackle the problem of money laundering at both the national and international levels. **(2021)**
2. Money laundering poses a serious security 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? **(2013)**

Process of Money Laundering

1	**Placement**	***Introduction of illegal funds into the financial system.***
2	**Layering**	*Concealing the source through complex transactions and transfers.*
3	**Integration**	*Reintroducing laundered money into the economy as legitimate funds.*

Techniques of Money Laundering

Technique	Description
Smurfing (Structuring)	Breaking large sums into smaller deposits to avoid detection/reporting.
Shell Companies	Using fake companies to show illicit money as legitimate income.
Trade-Based Laundering	Misrepresenting trade invoices to move money across borders.
Round Tripping	Circulating money through multiple jurisdictions and returning it as FDI.
Real Estate Investment	Buying properties with illicit funds to legitimise them through resale.
Hawala Transactions	Using informal channels to transfer money without physical movement.
Casinos and Gambling	Using gambling wins to show illegal earnings as prize money.
Digital Assets	Using cryptocurrencies to obscure transaction trails.

---

1. Reasons for Money Laundering

Reason	Description	Examples
1. Conceal Illicit Profits	Criminals launder money to hide proceeds from illegal activities such as *drug trafficking, extortion, or corruption,* making them appear legitimate.	*Sanjay Raut land scam case (2022):* ED alleged laundering of ₹1,034 crore in connection with the Patra Chawl redevelopment.
2. Tax Evasion	Individuals and businesses launder money to evade taxes by funnelling *undeclared income* through complex financial transactions or offshore accounts.	*Pandora Papers Leak (2021):* Exposed Indians holding offshore assets to evade taxes, including prominent business families.
3. Fund Criminal Activities	Laundered money is used to finance further illegal operations, including *terrorism, human trafficking, or organised crime,* without detection.	*2008 Mumbai Attacks:* Terror groups used hawala networks to launder funds for terrorist activities in India.
4. Circumvent Regulatory Oversight	Money laundering helps *bypass financial regulations,* such as anti-money-laundering (AML) laws, to move funds across borders undetected.	*Mahadev Betting App Scam (2023):* ₹6,000 crore allegedly laundered by using shell firms and fake identities.
5. Enhance Wealth and Lifestyle	Criminals launder money to *integrate illicit gains* into the economy, enabling lavish lifestyles or investments in legitimate businesses.	*Sahara India Case:* Funds from unregulated deposit schemes were laundered into real estate and other assets to project legitimacy.
6. Exploit Financial System Gaps	*Weak regulatory frameworks* or lax enforcement in certain jurisdictions are exploited to launder money through banks, real estate, or cooperatives.	*In India,* unregulated co-operative banks and benami properties are often used to launder black money, as seen in ED investigations.
7. Political Corruption	Politicians and officials often launder money to conceal bribes or misappropriate public funds, frequently through	*Jharkhand CM Hemant Soren Case (2024):* Alleged laundering of illegal mining proceeds through real estate and benami assets.

	shell companies or offshore accounts.	

2. Impact of Money Laundering

Impact Area	Description	Examples
1. Economic Distortion	Money laundering *distorts markets* by injecting illicit funds into legitimate sectors, inflating asset prices and undermining fair competition.*	In India, *benami properties in real estate,* funded by laundered money, have driven up property prices in cities like Mumbai and Delhi (ED reports, 2024).
2. Erosion of Financial System Integrity	Laundered funds *weaken trust* in financial institutions, increasing risks of fraud and regulatory violations in banks and markets.	*PNB-Nirav Modi scam 2018 (₹14,000 crore):* fake Letters of Undertaking damaged trust in India's banking sector.
3. Increased Crime and Corruption	Money laundering facilitates further criminal activities, including terrorism, drug trafficking, and corruption, by providing untraceable funds.	In 2025, *Delhi Police busted a global drug syndicate* operating across four continents and 10 + countries, funded via laundered cryptocurrency.
4. Revenue Loss to Government	Laundering enables tax evasion and siphoning of public funds, reducing government revenue for development and welfare projects.	*Panama Papers (2016):* revealed Indian entities evading tax through offshore accounts, costing the treasury crores in revenue (CBDT investigations).
5. Undermined Governance and Rule of Law	Laundered money fuels political corruption and weakens trust in governance and judicial systems.	*India & FATF Mutual Evaluation (2024):* highlighted vulnerabilities in the real estate and informal sectors, affecting its global financial standing.
6. Global Reputation Damage	Countries with high money laundering risks face reputational damage, deterring foreign investment and impacting economic growth.	*Sahara India Case:* laundered funds from unregulated deposit schemes diverted resources from small investors, widening economic inequality.
7. Social Inequality	Illicit funds concentrated in the hands of criminals exacerbate *wealth disparities,* undermining social equity and cohesion.	*Sahara India Case* — same context as above.
8. National Security Threats	Laundered money finances terrorism and organised crime, posing direct threats to internal and external security.	*Jammu & Kashmir Terror Funding (2019):* ED uncovered laundering networks channelling funds to separatist groups via hawala and cryptocurrencies.

3. Contribution of Emerging Technologies and Globalization to Money Laundering

Factor	Contribution to Money Laundering	Example
1. Cryptocurrencies	Provide *anonymity, decentralization,* and cross-border movement of funds with limited regulatory oversight, enabling crypto-based laundering.	In 2022, the ED traced ₹135 crore laundered via Bitcoin in a betting app scam run from China.
2. Online Banking & Fintech	Facilitate rapid, borderless fund transfers with inadequate KYC norms, enabling *regulatory arbitrage* and movement through shell accounts.	*Razorpay* flagged suspicious transactions linked to Chinese loan apps operating through shell fintech accounts.
3. Dark Web & Anonymous Platforms	Enable untraceable transactions, illicit trade, and peer-to-peer transfers beyond conventional law enforcement surveillance.	*Narcotics sold on the darknet* were paid for using Monero and Bitcoin, then routed through Indian crypto exchanges.
4. Virtual Assets & NFTs	Help in value obfuscation, price manipulation, and layering of illicit wealth using non-traditional digital assets.	*NFTs on OpenSea* were bought and resold between linked wallets to inflate prices and justify high-value crypto inflows.
5. Global Trade Networks	Involve trade-based money laundering (TBML) through *under/over-invoicing, false shipping documents,* and multi-jurisdictional complexity.	In 2021, *DRI unearthed over-invoicing* of mobile parts in a ₹1,000 crore trade-based laundering case involving UAE firms.
6. Offshore Financial Centres	Offer financial secrecy, low-tax jurisdictions, and lack of beneficial ownership transparency, aiding in *concealment and integration.*	*Panama Papers* revealed Indians using shell companies in the British Virgin Islands to hide illicit assets.
7. Freelancing & Gig Platforms	Misused for invoice manipulation, false service reporting, and placement of black money under the garb of freelance work.	*Fake graphic design jobs* posted on platforms like Upwork were used to invoice launder money from online gambling operations.

4. Challenges in Combating Money Laundering

Challenge	Description	Example
1. Compliance Burden	Financial institutions face high operational costs and resource strain to implement robust AML procedures, KYC, and monitoring systems.	In 2024, *RBI fined banks over ₹28 crore* for KYC lapses and data reporting failures.
2. Lack of Skilled Workforce	Shortage of trained AML professionals and low staff/public awareness impedes effective detection and reporting of laundering cases.	In 2025, *80 % of Indian employers reported difficulty finding skilled professionals.*
3. Legal Loopholes and Delays	Complex legal procedures, slow trials, and misuse of enforcement powers hinder timely conviction and confiscation of laundered assets.	*1,739 money laundering cases pending trial; only 47 PMLA cases decided (93 % conviction rate)* but significant procedural delays.
4. Technological Sophistication	Criminals use advanced digital tools, cryptocurrencies, and cross-border transactions to evade detection and regulatory oversight.	*Feb 2025:* ED seized ₹1,646 crore in cryptocurrency in a major money-laundering case.
5. Fragmented Enforcement	Multiple agencies with overlapping jurisdictions and poor coordination reduce effectiveness of AML enforcement efforts.	*Apr 2025:* FIU-IND and RBI signed MoU for enhanced information-sharing and coordination under PMLA.

5. Measures to Tackle Money Laundering

5.1 National Measures

Measure	Description
1. Prevention of Money Laundering Act (PMLA), 2002	Cornerstone AML law criminalising money laundering; empowers ED to attach, seize, and confiscate proceeds of crime. Amendments in 2019 and 2023 expanded scope to cryptocurrency platforms, NGOs, and politically exposed persons (PEPs).
2. Financial Intelligence Unit (India) – FIU-IND	Acts as central agency for receiving, analysing, and disseminating financial intelligence to ED, CBI, and RBI. Monitors suspicious transactions reported by banks and insurance firms.
3. Enforcement Directorate (ED)	Investigates and prosecutes offences under PMLA and FEMA; authorised to attach, seize, and confiscate assets.
4. Cryptocurrency Regulation Initiatives	30 % tax on Virtual Digital Assets (VDAs) since 2022; crypto platforms subject to AML reporting under FIU-IND.
5. Economic Intelligence Council (EIC)	High-level coordination body chaired by Finance Minister ensuring synergy among ED, CBI, CBDT, SEBI, and FIU.

6. Black Money (Undisclosed Foreign Income and Assets) Act, 2015	Targets undeclared foreign income with heavy penalties and prosecution; strengthens India's legal arsenal.
7. Benami Transactions (Prohibition) Amendment Act, 2016	Curbs benami property holdings by allowing confiscation under false names or proxies; complements PMLA in curbing asset laundering.

5.2 Global Measures

Measure	Description
1. Financial Action Task Force (FATF)	Inter-governmental body setting AML/CFT standards; India became member in 2010 and aligns domestic laws with 40 + 9 Recommendations.
2. Vienna Convention (1988)	First global treaty to recognise money laundering as crime linked to drug trafficking; enables asset seizure and mutual legal assistance.
3. Basel Committee Principles	Banking guidelines to prevent financial misuse through strong KYC, internal controls, and compliance audits.
4. Wolfsberg AML Principles	Private sector best practices adopted by global banks for ethical banking and high-risk client screening.
5. Egmont Group of FIUs	Global network of FIUs facilitating secure exchange of financial intelligence; India's FIU-IND is an active member.
6. UN Global Programme Against Money Laundering (GPML)	UNODC initiative providing training, legislative guidance, and technical assistance to developing countries. Hosts the International Money Laundering Information Network (IMoLIN).

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

Provision	Description
1. Definition of Money Laundering (Section 3)	Whosoever directly or indirectly attempts to indulge or knowingly assists or is party to 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 offence of money laundering.
2. Attachment of Property (Section 5)	ED may attach property suspected to be involved in money laundering for 180 days, subject to adjudicating authority confirmation.
3. Adjudicating Authority (Section 6)	Quasi-judicial body to decide whether attached property is involved in money laundering.
4. Appellate Tribunal (Section 25)	Hears appeals against orders of adjudicating authority.
5. Special Court (Section 43)	Designated court under PMLA to try offences of money laundering.
6. Confiscation (Section 8)	Once guilt is proved, proceeds of crime are confiscated to the Central Government.

7. Burden of Proof (Section 24)	Onus lies on the accused to prove that proceeds of crime are *untainted.*
8. Presumption in Interconnected Transactions (Section 23)	If one transaction is proved to involve money laundering, interconnected transactions are presumed to be involved as well.
9. Offences to be Cognizable and Non-bailable (Section 45)	Money laundering is *cognizable* and *non-bailable*; stringent bail conditions apply similar to TADA/POTA provisions.
10. Extraterritorial Jurisdiction (Section 56)	Applies to offences committed *outside India* involving property within India or Indian citizens abroad.

7. Enforcement and Implementation under PMLA

Institution / Measure	Role	Example / Remark
1. Enforcement Directorate (ED)	Investigates and prosecutes offences under *PMLA* and *FEMA*; empowered to attach properties, freeze bank accounts, and file prosecution complaints.	*ED attached ₹48,000 crore assets in FY 2024–25* in high-profile corruption and crypto-related cases.
2. Financial Intelligence Unit (FIU-IND)	Collects, analyses, and shares financial intelligence relating to suspicious transactions under PMLA.	*FIU fined Binance ₹18 crore (Jan 2025)* for AML violations.
3. National Economic Offence Records (NEOR) Database	Centralised repository for economic crimes, ensuring coordination between *CBI, ED, SFIO,* and *FIU.*	*Launched in 2024* to integrate data on high-risk entities and fraudsters.
4. Digital Forensics and AI Tools	Use of *AI-driven analytics, blockchain tracing,* and data mining tools to detect complex laundering networks.	*AI-based AML platform* piloted by *ED and NPCI* to track UPI-linked laundering networks.
5. Coordination with International Agencies	India collaborates with *Interpol, FATF, Egmont Group, and FIUs* for global intelligence sharing and extradition of economic offenders.	*Nirav Modi extradition case (UK)* highlights long-drawn procedural hurdles in mutual legal assistance.
6. Amendment (2023)	Expanded *"proceeds of crime"* to include *possession, acquisition, or use,* and extended applicability to cryptocurrency platforms, NGOs, and professionals like CAs/lawyers if found complicit.	*ED investigation against crypto exchange WazirX (2023):* First such case under extended definition.

8. FATF and India

Aspect	Details
1. FATF Mandate	Sets global AML/CFT (Anti-Money Laundering/Countering Financing of Terrorism) standards and monitors member countries for compliance.
2. India's Membership	India became a full member in *June 2010*; subject to mutual evaluation by FATF and Asia-Pacific Group on Money Laundering (APG).
3. FATF Recommendations	40 + 9 Recommendations forming global AML framework, covering areas such as *risk assessment, customer due diligence, PEP monitoring, asset freezing,* and *international cooperation.*
4. India's Compliance Status	As per *APG 2024 Mutual Evaluation Report*, India rated **"Compliant" in 12 areas** and **"Largely Compliant" in 20**, but *partially compliant* in *virtual asset regulation and beneficial ownership transparency.*
5. FATF Grey Listing	FATF urged India to improve mechanisms for *monitoring NPOs, cryptocurrency usage,* and *cross-border fund flows,* though India was **not grey-listed.**
6. FATF's New Mandate on Virtual Assets (2023)	Introduced *Travel Rule* compliance for Virtual Asset Service Providers (VASPs) and mandated real-time fund origin tracking.
7. FATF Mutual Evaluation (2025–26)	India's upcoming evaluation will assess compliance with FATF's 2023 standards; key focus areas: *crypto regulation, PEP monitoring,* and *cross-border cooperation.*

---

9. Judicial Interpretations

Case	Verdict / Significance
Vijay Madanlal Choudhary v. Union of India (2022)	Upheld constitutional validity of *PMLA*, including powers of *ED to arrest, attach, and conduct search/seizure without FIR.* Recognised money laundering as a serious economic offence.
Kartar Singh v. State of Punjab (1994)	Established that stringent bail provisions in anti-terror laws must balance individual liberty and national security — relevant for *PMLA bail interpretation.*
Nikesh Tarachand Shah v. Union of India (2017)	Struck down *Section 45(1)* bail conditions as unconstitutional for violating *Article 14 and 21*, leading to legislative amendment reinstating similar provisions in 2018.
P. Chidambaram v. ED (2019)	Supreme Court upheld ED's authority under *PMLA* to ensure thorough investigation of economic offences, stressing national security implications.
Ratul Puri v. Directorate of Enforcement (2022)	Reiterated that *mere delay in trial does not entitle bail* under PMLA given the gravity of the offence.

Satyendar Jain v. Directorate of Enforcement (2024)	Delhi HC ruled ED must prove *conscious possession* of proceeds of crime; reinforced procedural fairness in attachment and arrest under PMLA.

10. Way Forward

Strategy	Description
1. Strengthen Inter-Agency Coordination	Establish *National Economic Offences Coordination Centre (NEOCC)* for real-time data exchange among *ED, FIU, SFIO, and RBI.*
2. Enhance AML Workforce & Training	Introduce *specialised AML training academies* and expand capacity of *FIU-IND* and banks' compliance divisions.
3. Regulate Cryptocurrencies and Virtual Assets	Implement *comprehensive regulatory framework* for VDA exchanges under *PMLA* and ensure real-time monitoring.
4. Improve Beneficial Ownership Transparency	Mandate *public beneficial ownership registers* for companies and trusts to curb shell entities.
5. Judicial Reforms & Fast-Track Courts	Establish *special PMLA courts* for quicker trial and disposal of money laundering cases.
6. Strengthen Data-Sharing with Global Agencies	Leverage *Egmont Secure Web (ESW)* and *Interpol* for real-time intelligence sharing and extradition of offenders.
7. Public Awareness and Financial Literacy	Promote citizen awareness on *AML norms, crypto risks,* and *reporting suspicious activities.*
8. Ethical Corporate Governance	Encourage companies to implement *Know Your Beneficiary (KYB)* and *Anti-Bribery Management Systems (ISO 37001).*
9. Technological Vigilance	Deploy *AI-driven analytics, blockchain tracing, and RegTech tools* for early detection of suspicious transactions.
10. International Cooperation	Collaborate through *FATF, G20, IMF,* and *World Bank* for harmonised AML policies and cross-border legal assistance.

Conclusion:
Money laundering is not just an economic offence but a direct threat to **national security, governance, and integrity.**
While India's *PMLA framework* and *FATF compliance* mechanisms have evolved, challenges persist in the form of *cryptocurrency misuse, judicial delays, and inter-agency coordination.*
As **Prime Minister Narendra Modi** asserted during the *G20 Summit (2023)*, *"Global cooperation against financial crimes must match the borderless nature of money laundering and terror financing."*

A **holistic, technology-driven, and globally harmonised approach** is essential to safeguard India's financial sovereignty and internal security.

3.4 Security challenges and their management in border areas; linkages of organized crime with terrorism

Border Management

Border management in India is a **multidimensional security function** involving the regulation of *legal and illegal movement of people and goods, prevention of infiltration, smuggling, and cross-border crimes,* and development of border regions.

The **Ministry of Home Affairs** defines it as *"securing borders against hostile interests while facilitating trade and travel."*

India has a **vast land border of 15,106.7 km and a coastline of 11098 km**, sharing borders with **seven countries** by land:
Bangladesh (4096.7 km), China (3488 km), Pakistan (3323 km), Nepal (1751 km), Myanmar (1643 km), Bhutan (699 km), and Afghanistan (106 km).

UPSC Previous Year Questions

1. India has a long and troubled border with China and Pakistan, fraught with contentious issues. Examine the conflicting issues and security challenges along the border. Also, give out the development being undertaken in these areas under the Border Area Development Programme (BADP) and Border Infrastructure and Management (BIM) Scheme. *(2024)*
2. 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. *(2023)*
3. What are the maritime security challenges in India? Discuss the organisational, technical, and procedural initiatives taken to improve maritime security. *(2022)*
4. Analyse internal security threats and transborder crimes along Myanmar, Bangladesh and Pakistan borders, including the Line of Control (LoC). Also, discuss the role played by various security forces in this regard. *(2020)*

5. For effective border area management, discuss the steps required to be taken to deny local support to militants, and also suggest ways to manage a favourable perception among locals. *(2020)*
6. 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 countermeasures should be taken to prevent the same? *(2018)*
7. Border management is a complex task due to difficult terrain and hostile relations with some countries. Elucidate the challenges and strategies for effective border management. *(2016)*
8. In 2012, the longitudinal marking for high-risk areas for piracy was moved from 65 degrees east to 78 degrees east in the Arabian Sea by the International Maritime Organisation. What impact does this have on India's maritime security concerns? *(2014)*
9. China and Pakistan have entered into an agreement for development of an economic corridor. What threat does this pose for India's security? Critically examine. *(2014)*
10. International civil aviation laws provide all countries complete and exclusive sovereignty over the airspace above their 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 suggest ways to contain the threat. *(2014)*
11. How far are India's internal security challenges linked with border management, particularly in view of the long porous borders with most countries of South Asia and Myanmar? *(2013)*

---

1. Need for Border Management in India

Reason	Description	Example
1. National Security	Prevents infiltration, terrorism, and arms/drug trafficking by hostile actors, ensuring sovereignty and safety.	*Pahalgam terror attack:* Pakistan-based terrorists infiltrated via LoC and killed 26 innocent civilians.
2. Demographic Stability	Controls illegal immigration, prevents demographic shifts, and maintains social balance in border regions.	*NRC in Assam:* Over 19 lakh excluded due to illegal immigration concerns.
3. Social Harmony	Peaceful border communities prevent trafficking and cross-border crimes, protecting vulnerable groups as India remains a key trafficking hub.	*India-Nepal anti-trafficking efforts* include **SSB-APF collaboration**, rescues, NGO support, and awareness campaigns to prevent human trafficking and foster social harmony.
4. Sovereignty & Territorial Integrity	Upholds international boundaries, deters encroachment, and asserts state	*2020 Galwan clash:* PLA incursion in Ladakh challenged Indian territorial integrity.

	authority in disputed or sensitive areas.	
5. Development & Connectivity	Promotes infrastructure, welfare, and connectivity in remote border areas, reducing alienation and outmigration.	*Vibrant Villages Programme (2023):* 663 border villages targeted for all-weather connectivity.
6. Narco-terrorism	Checks insurgency, arms flow, and narco-terrorism, especially in Northeast and Punjab, through robust policing.	*Punjab Police's counter-intelligence unit* uncovered a drug smuggling network linked to Pakistan-based operatives, recovering 5 kg of heroin.
7. Maritime Security	Secures vast coastline from piracy, smuggling, illegal migration, and terror infiltration via sea routes.	*Indian Coast Guard and ATS Gujarat* joint operation intercepted Indian fishing boat at sea and seized 173 kg of narcotics.

2. Challenges in Border Management in India

Challenge	Description	Example
1. Porous & Difficult Terrain	Borders traverse deserts, dense forests, rivers, and high mountains, complicating surveillance and fencing efforts.	*81.5% of India–Bangladesh border* (900+ km of riverine stretch) remains highly porous.
2. Infrastructure Deficit	Lack of all-weather roads, bridges, and border outposts hinders troop mobility, logistics, and quick response.	*Trans-Arunachal Highway, East-West Corridor* face delays; many roads 60–80 km short of LAC.
3. Manpower Shortage	Significant vacancies in CAPFs and Assam Rifles impact effective patrolling and area dominance.	*83,127 posts vacant in CAPFs/Assam Rifles* against 10 lakh sanctioned strength as of Jan 2023.
4. Cross-Border Crime & Smuggling	Smuggling of drugs, arms, cattle, and human trafficking thrives due to porous borders and local collusion.	*Fourfold rise in Bangladesh apprehensions (2018–2022):* ₹1,200 crore drugs seized in Punjab (2024).
5. Illegal Immigration & Demographic Changes	Unchecked migration alters local demographics, strains resources, and triggers social tension in border states.	*Assam NRC anti-foreigner agitation*; demographic shifts in West Bengal and Tripura (NCRB, 2024).
6. Border Disputes & Hostile Neighbours	Unresolved boundaries with China, Pakistan, and Nepal cause frequent standoffs, infiltration, and diplomatic strain.	*Galwan clash (2020)* with China; *2023 ceasefire violations* by Pakistan; *Kalapani dispute* with Nepal.

7. Environmental & Civil Liberties Concerns	Strategic projects and surveillance raise deforestation, displacement, and privacy issues in ecologically sensitive zones.	*Forest (Conservation) Amendment Act, 2023* exempts projects within 100 km of border, raising ecological alarms.

3. India–China Border Challenges

Category	Details
1. Unresolved Boundary Dispute	The Line of Actual Control (LAC) is undemarcated and contested in the *Western (Aksai Chin)* and *Eastern (Arunachal Pradesh)* sectors. Multiple perceptions of LAC lead to frequent standoffs *(Galwan clash 2020, Tawang 2022).*
2. Asymmetrical Infrastructure	China has superior border infrastructure—roads, tunnels, airstrips facilitating swift troop mobilisation. India lags, especially in Arunachal and Ladakh.
3. Dual Command Structure	Border areas guarded by **ITBP (under MHA)** and **Army (under MoD)**, creating coordination issues during crises.
4. Aggressive Chinese Posture	"Salami slicing" tactics and expansionist designs *(Doklam 2017)* challenge India's territorial integrity.
5. Water Security Concerns	*China's dam-building on Brahmaputra* raises fears of water flow manipulation, ecological degradation, and lack of data-sharing.
6. Surveillance Deficiency	In high-altitude areas, India faces challenges in continuous surveillance due to terrain and weather.
7. Cyber & Information Warfare	Chinese cyber threats, GPS spoofing, and info warfare pose new layers of challenges.

3.1 Measures Taken by Government for Border Management with China

Measure	Details
1. Infrastructure Development	Strategic roads like **DS-DBO Road, Sela Tunnel, Frontier Highway** in Arunachal to enhance troop movement.
2. Vibrant Villages Programme (2023)	Implemented in 46 blocks of 4 border states to prevent migration, enhance livelihood, and promote border security via civilian presence.
3. Military Modernisation & Realignment	Forward deployment, creation of new **mountain strike corps**, logistics hubs in Ladakh & Arunachal.
4. Comprehensive Surveillance (CIBMS)	Use of **UAVs (Heron)**, night vision, satellite imagery, and motion sensors for LAC monitoring.
5. Border Roads Organisation (BRO) Initiatives	Projects like **Chardham Mahamarg, DSDBO Road**, airstrips at Nyoma, Daulat Beg Oldi for rapid mobilisation.

6. Confidence Building Measures (CBMs)	Series of agreements: *1993 (Peace & Tranquillity), 1996 (CBMs Protocols), 2013 (Border Defence Cooperation Agreement).*
7. Diplomatic Engagement Mechanisms	*Working Mechanism on Border Affairs (WMCC)* and *Special Representatives (SR) Dialogue* to resolve LAC tensions.
8. Strengthening QUAD and Defence Partnerships	Enhanced Indo-US logistics and deepened diplomacy to counterbalance Chinese influence.
9. Technology Use for Monitoring	AI-based surveillance, long-range cameras, and automated observation posts along high-altitude sectors.

4. India–Pakistan Border Challenges

Category	Details
1. Cross-Border Terrorism	Persistent threat due to **state-sponsored terrorism** from Pakistan. Terror groups like *Lashkar-e-Taiba (LeT)* and *Jaish-e-Mohammed (JeM)* operate under ISI patronage. **Major incidents:** Uri (2016), Pulwama (2019). Classified under *asymmetric warfare* and a core *non-traditional security threat.*
2. Ceasefire Violations	Regular Line of Control (LoC) shelling undermines the **2003 ceasefire agreement.** Used as *cover fire* for infiltration by terrorists. Impacts border area civilians, increases *psychological insecurity,* and disturbs the *internal security architecture* in J&K.
3. Narco-Terrorism & Drone Infiltration	Drones used to drop heroin, AK-47s, IEDs, and fake documents across the Punjab border, signifying the **convergence of crime and terrorism.** Over 100 drone sightings recorded in 2023. Part of the *emerging hybrid threats landscape.*
4. Unresolved Border Disputes	Disputes like **Siachen, Sir Creek,** and the continued illegal occupation of **Pakistan-occupied Kashmir (PoK).** *Sir Creek dispute* affects maritime boundary demarcation and India's **Exclusive Economic Zone (EEZ)** in the Arabian Sea.
5. Smuggling and FICN Infiltration	Constant inflow of **Fake Indian Currency Notes (FICN), gold, and weapons** from across the border. FICN is considered *economic subversion and economic terrorism* under India's security framework.
6. Porous Terrain in Western Border	Riverine gaps, desert dunes, and marshy terrain in states like Gujarat and Rajasthan allow cross-border crime. These vulnerabilities are exploited by both state and non-state actors.
7. Radicalisation of Border Youth	Exposure to **cross-border propaganda, hate speech, and digital radicalisation** tactics indoctrinates youth, creating *internal security fragility* in border states.

4.1 Measures Taken by Government for Border Management with Pakistan

Measure	Details
1. Smart Fencing (CIBMS)	*Comprehensive Integrated Border Management System* uses **thermal sensors, infrared cameras, fibre-optic detection, and laser walls.** Deployed in Jammu and Punjab sectors.
2. Anti-Drone Infrastructure	**Drone jammers, RF signal interceptors, and quick reaction teams (QRTs)** deployed in Punjab and Gurdaspur sectors to counter UAV threats.
3. Modernisation of Border Outposts (BOPs)	High-mast surveillance towers, night-vision devices, and fortified shelters to enhance *forward defence posture.*
4. Strategic Border Road Development	Under **BIM Scheme**, roads and fencing in deserts (Samba, Rajasthan) and Sir Creek sectors enhance preparedness.
5. UAV and Aerial Surveillance Systems	UAVs like **Heron, Rustom-II, and quadcopters** deployed for day/night aerial patrols.
6. Integrated Check Posts (ICPs)	ICPs at **Attari (Punjab)** support *legal trade and human movement* while strengthening customs and immigration surveillance.
7. 2021 Ceasefire Reaffirmation	The **DGMO-level reaffirmation (Feb 2021)** reduced cross-border firing significantly, signalling *strategic restraint.*
8. Multi-Agency Coordination	Regular coordination among **BSF, IB, RAW, NIA, and state police** via **MACs (Multi-Agency Centres)** for counter-infiltration grids.
9. Coastal & Creek Area Security	Gujarat's *Sir Creek* area patrolled by **BSF marine radars and water wings** under the **Sagar Kavach** and **Coastal Security Scheme.**
10. Bilateral Institutional Mechanisms	Engagement via **hotlines, flag meetings, and BSF–Pak Rangers coordination** meetings to maintain communication and avoid escalation.

5. India–Bangladesh Border Challenges

Category	Details
1. Porous and Complex Terrain	India's **4,096 km border** with Bangladesh is the *longest land boundary*, passing through rivers, forests, and densely populated villages, leading to *frequent illegal crossings and smuggling.*
2. Illegal Migration & Identity Fraud	*Demographic pressure* and economic disparity drive **illegal immigration** into Assam, West Bengal, and Tripura. Migrants are vulnerable to *fake ID networks*, creating *internal demographic insecurity.*
3. Cattle and Narcotics Smuggling	India is a *source country* for cattle smuggled into Bangladesh; drugs like *Phensedyl syrup* and *Yaba pills* are smuggled into India, fuelling *cross-border crime.*
4. Violence and Attacks on BSF	Increasing incidents of **cross-border aggression**; BSF personnel attacked by armed smugglers *(Cooch Behar 2022).*

5. Fence Breach and Infrastructure Gaps	Around **150 km of border remains unfenced** due to land issues and opposition, creating *border management blind spots.*
6. Transnational Human Trafficking	India–Bangladesh border acts as a *destination and transit route* for human trafficking; women and children trafficked for labour and sexual exploitation.
7. Overlapping Local Livelihood Interests	Farmers and traders rely on informal border trade; restrictions create resistance to border formalisation.
8. Fake Indian Currency Notes (FICN)	FICN infiltrates from Bangladesh as part of **economic destabilisation and terror financing.**

5.1 Measures Taken by Government for Border Management with Bangladesh

Measure	Details
1. Fencing and Floodlighting	88% of fencing (around 3,326 km) completed; remaining stretches use *floating fences and sensor-based barriers* under **BIM Scheme.** Floodlighting used for *night-time breach prevention.*
2. Comprehensive Integrated Border Management System (CIBMS)	*Electro-optic sensors, radars, infrared cameras* deployed in Assam and Bengal riverine zones for real-time monitoring.
3. Deployment of BSF and Force Modernisation	BSF units equipped with *non-lethal weapons, body-worn cameras,* and *GPS trackers.*
4. ICPs and Legal Trade Facilitation	ICPs at **Petrapole (WB), Agartala (Tripura), Dawki (Meghalaya)** streamline legal trade and reduce illegal infiltration.
5. Joint Coordination with Border Guards Bangladesh (BGB)	Regular **flag meetings, joint patrolling,** and hotline communication for trust and de-escalation.
6. Border Area Development Programme (BADP)	Roads, schools, and health infrastructure improved; aligned with **Vibrant Villages Strategy** for inclusive development.
7. Counter-Trafficking Operations	Joint action between **BSF, NIA, NCW, NGOs** to tackle *child trafficking rings.* Surveillance strengthened at *Dhaka–Kolkata route.*
8. Use of UAVs and Technology Surveillance	Drones and ground sensors used in **Murshidabad, Malda, Karimganj** sectors for *real-time monitoring.*
9. Legal Framework & Soft Borders	Citizenship laws, Foreigners Tribunals, and fencing adjusted to prevent alienation while maintaining *sovereignty enforcement.*
10. People-Centric Engagement	*Bharat–Bangla Maitri initiatives* promote cultural and trade ties, building trust among border communities.

6. India–Nepal Border Challenges

Category	Details
1. Open Border System	1,751 km long open border under the **1950 Indo–Nepal Treaty** allows visa-free movement but facilitates *unauthorised migration, smuggling,* and *cross-border crime.*
2. Territorial Disputes	The **Kalapani–Limpiyadhura–Lipulekh dispute** escalated after Nepal's 2020 map revision, raising sovereignty issues.
3. Smuggling & Informal Trade	Open border enables *unregulated trade* in gold, electronics, and timber, creating transnational black markets.
4. Fake Indian Currency Network (FICN)	Nepal used as *transit route* by ISI-linked FICN operatives.
5. Terrorist Infiltration Route	*Lightly guarded open border* exploited by *Pakistani and Bangladeshi operatives.* Recognised as *non-conventional infiltration route.*
6. Human Trafficking & Security Gaps	Nepal is a *source country* for women/children trafficked into India; weak biometric checks exacerbate issue.
7. Local Resistance to Regulation	Tightening border control faces resistance due to livelihood and kinship ties.
8. Insufficient Infrastructure	Sparse SSB posts and poor roads limit response time in Terai region.

6.1 Measures Taken by Government for Border Management with Nepal

Measure	Details
1. Deployment of Sashastra Seema Bal (SSB)	SSB is designated **frontier guarding force** for Indo–Nepal border, maintaining community networks for *non-intrusive vigilance.*
2. Fencing and Selective Border Regulation	Pilot fencing in sensitive sectors of *Bihar and UP* with high FICN activity.
3. Integrated Check Posts (ICPs)	ICPs at **Raxaul, Jogbani, Biratnagar, Sonouli** regulate trade and migration.
4. Joint Technical Mechanisms	*India–Nepal Boundary Working Group (BWG)* addresses boundary demarcation and encroachments.
5. BADP and Infrastructure Development	BADP invests in *roads, schools, water supply* in border villages.
6. Intelligence Sharing	Real-time flow between **SSB, IB, RAW, and Nepal Police**; use of *mobile surveillance and digital checklists.*
7. Bilateral Coordination	*District-level coordination* between Indian and Nepalese officers for *community-level confidence building.*
8. Use of Technology & Biometric Verification (Pilot)	Biometric systems at **Raxaul, Jogbani** to track high-risk entrants.
9. Capacity Building & Training	Joint training for *border personnel, counter-smuggling,* and *human rights-based policing.*

10. Soft Diplomacy & People-Centric Initiatives	Cultural, educational, and visa facilitation programmes promote *social cohesion* in sensitive zones.

7. India–Bhutan Border Challenges

Category	Details
1. Inaccessible & Rugged Terrain	The 699 km border runs through *Himalayan forests*, posing *geospatial surveillance challenges.*
2. Chinese Strategic Encroachment	*2017 Doklam standoff* highlighted China's threat to **Siliguri Corridor (Chicken's Neck)** — India's strategic chokepoint.
3. Cross-Border Movement of Insurgents	ULFA, NDFB, KLO groups from Northeast found *shelter in Bhutanese jungles.*
4. Limited Security Infrastructure	Bhutan's limited border surveillance capacity creates *security asymmetry.*
5. Smuggling & Illicit Trade	Smuggling of *timber, drugs, and consumer goods* through Assam–Bhutan border areas.
6. Environmental Security Concerns	Illegal logging and wildlife trafficking threaten *Manas Reserve.*
7. Civilian Sensitivities & Ethnic Proximity	Shared ethnic ties (Bodo–Bhutanese) demand *humane, sensitive security operations.*

7.1 Measures Taken by Government for Border Management with Bhutan

Measure	Details
1. Bilateral Security Partnership	*2007 India–Bhutan Friendship Treaty* ensures joint **logistical, training, and tech support** to Bhutan Army.
2. Doklam Intervention (2017)	India's intervention at *Jampheri ridge* stopped PLA construction, strengthening deterrence.
3. Deployment of SSB & Army Coordination	SSB guards Assam, Sikkim, and Arunachal sectors; coordinated with *Army Eastern Command.*
4. BRO Projects	Roads like *Gelephu–Samdrup Jongkhar* enhance *infrastructure diplomacy.*
5. Coordinated Counter-Insurgency Ops	*Operation All Clear (2003–04)* eliminated ULFA, NDFB hideouts, showing *cross-border cooperation.*
6. Surveillance Infrastructure	*High-altitude posts, satellite imagery,* and ground intel in *Darrang, Samdrup, Phuentsholing.*
7. Border Haats & People Exchange	Trade haats facilitate livelihood security near *Kalikhola* and *Samtse.*
8. Joint Training & Capacity Building	Regular *SSB–RBA exchanges* for interoperability.
9. Environmental Security Cooperation	Joint conservation of *Manas Wildlife Sanctuary.*
10. Strategic Resilience in Siliguri Corridor	Focus on *surveillance, infrastructure,* and *rapid deployment* due to corridor criticality.

8. India–Myanmar Border Challenges

Category	Details
1. Porous & Difficult Terrain	1,643 km border runs through *dense forests and rugged hills* in Arunachal, Mizoram, Manipur, Nagaland — making surveillance difficult.
2. Free Movement Regime (FMR) Misuse	FMR allows ethnic tribes (Nagas, Kukis, Chins) to move 16 km visa-free; exploited by *insurgents and traffickers.*
3. Cross-Border Insurgency	Groups like *NSCN(K), ULFA(I), PLA, PREPAK* use *safe havens in Myanmar* to regroup and attack Indian territory.
4. Drug & Arms Trafficking	Proximity to the *Golden Triangle* makes this region a hub for heroin and Yaba trafficking.
5. Refugee Influx & Ethnic Tensions	*Post-2021 Myanmar coup,* Chin & Kuki refugees entered India, creating humanitarian dilemmas.
6. Weak Institutional Presence	Sparse *SSB/Assam Rifles* infrastructure limits response; terrain delays mobilisation.
7. Undermining of Border Sovereignty	Unregulated trade and movement weaken *state legitimacy* in frontier zones.

8.2 Measures Taken by Government for Border Management with Myanmar

Measure	Details
1. Suspension & Review of FMR	FMR *temporarily suspended in Manipur (2023)* due to insurgency; India reviewing terms for national security balance.
2. Border Fencing Projects (2024 onwards)	*10 km fencing pilot in Manipur* under way; hybrid model with *smart sensors and physical barriers.*
3. Deployment of Assam Rifles & Force Modernisation	Assam Rifles equipped with *modern surveillance gear, UAVs, GPS tracking* for counter-insurgency.
4. Joint Military Operations: Sunrise I & II	Joint Indo–Myanmar ops (2019–20) targeted NSCN(K), ULFA(I), NDFB camps — *examples of cross-border counter-insurgency cooperation.*
5. Border Infrastructure & Roads (BADP/BIM)	Investment in *helipads, roads, culverts* under border schemes for troop access.
6. Development of Integrated Check Posts (ICPs)	**ICP Moreh (Manipur)** upgraded for trade regulation and migration control.
7. Technology-Enabled Surveillance	Use of *drones, thermal imaging, night vision* in *Chandel, Ukhrul, Champai* for pre-emptive detection.
8. Ethnic Reconciliation & Community Engagement	Outreach through *tribal leaders, border schools,* and medical camps to reduce insurgent recruitment.
9. Refugee Management & SOPs	*MHA issued biometric registration guidelines (2021–22)* for refugees; balanced security–humanitarian approach.

10. Strategic Cooperation with Myanmar Military (Tatmadaw)	India engages with Tatmadaw under *"Act East" and Pragmatic Engagement Policy"* to sustain operational coordination.

9. Issues in Border Management with Sri Lanka

Category	Details
1. Maritime Nature of the Border	India–Sri Lanka share a **maritime boundary of ~400 km** in the *Palk Strait, Gulf of Mannar,* and *Bay of Bengal.* This **sea-based boundary** poses distinct challenges such as *fishermen's conflict, piracy,* and *illegal maritime trade,* unlike traditional land borders.
2. Katchatheevu Island Dispute	The **ceding of Katchatheevu Island to Sri Lanka (1974)** without parliamentary ratification remains a point of **legal and political contention.** It affects **sovereign maritime rights** and is often raised in Tamil Nadu politics.
3. Fishermen Disputes and Arrests	Indian fishermen from Tamil Nadu often cross into Sri Lankan waters due to unclear demarcations or resource depletion. This leads to **frequent arrests, boat seizures,** and occasionally **firing by the Sri Lankan Navy,** escalating *bilateral tension* and humanitarian concerns.
4. Human Trafficking and Illegal Migration	The Tamil Nadu coast has seen waves of **Sri Lankan Tamil refugees** since the civil war era. Recently, the economic crisis in Sri Lanka (2022–23) triggered renewed **illegal migration and refugee influx,** straining *coastal security and humanitarian management.*
5. Smuggling and Maritime Terrorism Risk	Smuggling of **gold, narcotics (meth, cannabis), and weapons** across Palk Bay poses a challenge. Proximity to former **LTTE networks** still raises concerns of *residual terrorism, arms movement,* and *radicalisation threats.*
6. Inadequate Maritime Surveillance	Shallow waters, small islands, and a lack of persistent aerial surveillance lead to gaps in **maritime domain awareness (MDA),** especially in the *Gulf of Mannar and Rameswaram coast.*
7. Shared Ethnic and Cultural Ties	Close ethnic ties between **Indian Tamils and Sri Lankan Tamils** result in *dual identity complexities,* making enforcement of migration laws and repatriation politically sensitive.

9.1 Measures Taken by Government for Border Management with Sri Lanka

Measure	Details
1. Coastal Surveillance & Joint Patrolling	India and Sri Lanka conduct **coordinated naval patrols (CORPATs)** to monitor *Illegal, Unreported, and Unregulated (IUU) fishing, smuggling,* and *suspicious vessels.* Enhances **maritime domain awareness (MDA).**

2. Coastal Security Scheme (CSS)	India has strengthened **coastal police stations, marine police, radar stations,** and **automatic identification systems (AIS)** along the Tamil Nadu coast under CSS Phases I & II, enhancing **coastal border resilience.**
3. Installation of Chain of Static Sensors	**Indian Coast Guard (ICG)** installed a network of **coastal radars, AIS receivers,** and **VHF communication towers** to monitor shallow and deep-sea activity in *Palk Bay and Gulf of Mannar.*
4. Modernisation of Fishermen Tracking Systems	Use of **Vessel Monitoring Systems (VMS), biometric ID cards for fishermen,** and GPS-enabled boats helps track and verify legitimate fishing vessels. Supports **civilian maritime security architecture.**
5. Humanitarian Refugee Management	Camps in Tamil Nadu host **58,000+ Sri Lankan Tamil refugees (as of 2023).** India ensures human rights compliance, biometric registration, and periodic review of **voluntary repatriation mechanisms.**
6. Diplomatic Engagement on Fishermen Issue	High-level bilateral meetings (*Joint Working Groups*) between India and Sri Lanka to resolve **fishermen detention, propose joint fishing zones,** and **phase out bottom trawling.**
7. Operation SAGAR & SAGAR Doctrine	India's **Security and Growth for All in the Region (SAGAR)** vision includes **capacity-building and security assistance** to Sri Lanka, including *naval vessels, patrol craft, and surveillance equipment.*
8. Coastal Community Engagement	Initiatives like *Sea Vigil,* awareness programs, and fishermen training build **civilian cooperation** in intelligence gathering and promote **community-based border policing.**
9. Katchatheevu Legal Review Proposals	Calls for legal and diplomatic review of **Katchatheevu agreement (1974)** to reclaim traditional fishing rights and ensure **maritime sovereignty** in Tamil Nadu.
10. India–Sri Lanka Integrated Maritime Framework	Ongoing discussions on a **Common Maritime Boundary Regime, maritime delimitation agreements,** and **blue economy collaboration** promote long-term **strategic maritime stability.**

10. Maritime Border Management

10.1 Maritime Security Challenges in India

Category	Details
1. Piracy and Sea Lanes Threats	Threats from piracy in the Arabian Sea and the Gulf of Aden, especially affecting Indian merchant vessels. Disruption of Sea Lines of Communication (SLOCs) threatens energy and trade security.

2. Maritime Terrorism	Post-26/11 Mumbai attacks, sea-borne infiltration by terrorists became a critical threat. India's ≈11098 km coastline is vulnerable to non-state actor incursions, particularly via fishing vessels.
3. Smuggling and Contraband Trafficking	Sea routes are exploited for arms, narcotics, gold, and human trafficking. Coastal states like Gujarat and Kerala report seizures, indicating active transnational crime networks.
4. Illegal, Unreported, and Unregulated (IUU) Fishing	Unauthorised fishing by foreign vessels leads to resource depletion and conflicts (such as the India–Sri Lanka fishermen conflict). It undermines maritime economy security.
5. Geo-strategic Competition	Chinese naval presence in the Indian Ocean Region (IOR) through dual-use ports (such as Gwadar, Hambantota) and PLA Navy (PLAN) submarines raises strategic encirclement risks under the String of Pearls theory.
6. Maritime Boundary Disputes	Unresolved issues like Sir Creek (Pakistan) and historical concerns like Katchatheevu (Sri Lanka) create grey zones, leading to local conflicts and diplomatic challenges.
7. Lack of Maritime Domain Awareness (MDA)	India's vast Exclusive Economic Zone (EEZ) of ≈2.3 million sq. km lacks comprehensive real-time surveillance due to limited sensor coverage and coordination gaps among agencies.
8. Natural Disasters and Climate Risks	Coastal infrastructure and naval bases are increasingly at risk due to cyclones, sea-level rise, and tsunamis, impacting maritime resilience and disaster response.

10.2 Organisational, Technical, and Procedural Initiatives for Strengthening Maritime Security

Initiative Type	Details
1. Organisational	**Three-tier Security Architecture – Post-26/11, Navy (beyond 12 NM), Coast Guard (up to 12 NM), and State Marine Police (0-5 NM)** share roles, though UNCLOS doesn't recognise 0-5 NM separately, causing jurisdictional overlap within territorial waters. **National Committee on Strengthening Maritime and Coastal Security (NCSMCS)** – *Apex coordination body*, chaired by the Cabinet Secretary, comprising central and state agencies to address policy, operational, and capacity issues. **Information Management and Analysis Centre (IMAC)** – Established in Gurugram for real-time data fusion and analysis from multiple maritime sources. Central to India's MDA (Maritime Domain Awareness) framework. **National Maritime Security Coordinator (NMSC)** – New post under NSA to ensure inter-agency coordination across the Navy, Coast Guard, Customs, intelligence, and shipping sectors. Proposed in 2021.
2. Technical	**Coastal Radar Chain – Coastal surveillance radar stations** cover Indian and friendly IOR nations. These radars detect non-AIS-compliant vessels and enhance early warning capabilities.

	Automatic Identification System (AIS) – *Mandatory installation* on vessels over 20 metres to track position, speed, and ID. Helps authorities distinguish legitimate and suspicious vessels. **National Automatic Identification System (NAIS)** – A pan-India system to integrate AIS data from all coasts and islands. It is integrated into IMAC for real-time vessel tracking. **Satellite-Based Surveillance – Use of RISAT, Oceansat, and commercial satellites** for wide-area maritime monitoring, including piracy hotspots and EEZ tracking.
3. Procedural	**Coastal Security Scheme (CSS) Phases I & II –** Launched in 2005 and expanded, focusing on setting up *marine police stations, interceptor boats,* and training coastal police in 9 coastal states and 4 UTs. **SAGAR Vision (Security and Growth for All in the Region)** – India's maritime strategy to ensure regional security cooperation, capacity-building, and presence in IOR. Links economic security to strategic security. **International Cooperation – Regular CORPATs (Coordinated Patrols)** with Indonesia, Thailand, Sri Lanka, Seychelles, and QUAD exercises to project presence and secure IOR. **Sea Vigil and Theatre-Level Exercises** – *Biennial pan-India maritime security exercise 'Sea Vigil'* simulates threats and tests readiness. Supported by *TROPEX (Theatre-level Readiness Operational Exercise)* led by the Navy.

11. Air Space Management

11.1 Airspace Management Issues in India

Category	Details
1. Civil–Military Airspace Segregation	India follows a *segregated airspace model*, where military and civilian flights operate under separate controls. This leads to *inefficiency, flight delays,* and underutilisation of national airspace.
2. Congested Air Corridors and Urban Airspace	Key urban centres like Delhi, Mumbai, and Bengaluru face airspace congestion, increasing ATC workload, delays, fuel consumption, and risk of near-miss events.
3. Limited Real-Time Airspace Flexibility	Lack of dynamic airspace allocation affects emergency responses and optimised flight routing, especially during *natural disasters or VIP movements.*
4. Unregulated Drone/UAV Traffic	Rise in low-cost UAVs and drones for commercial, recreational, and surveillance purposes without adequate air traffic integration creates low-altitude airspace vulnerabilities. Also raises risk of terrorist misuse, as seen in *drone drops near border regions (such as Punjab).*

5. Security Risks near the Border and Sensitive Installations	Airspace near military zones, nuclear installations, and border areas often lacks comprehensive low-level surveillance, risking unauthorised aerial intrusions (*such as the Pathankot Airbase attack, 2016*).
6. Air Defence Identification Zones (ADIZ) Not Fully Operationalised	India lacks a fully integrated ADIZ framework, essential for early detection and classification of unidentified or rogue aircraft in strategic sectors.
7. Lack of Unified Airspace Management Authority	*Multiple agencies* (AAI, IAF, DGCA, DRDO, Home Ministry) operate in silos, leading to coordination gaps, especially in real-time threat scenarios or high-altitude security events.
8. Technological Gaps in Surveillance	Despite radar coverage in major zones, radar blind spots, lack of ADS-B systems, and satellite-aided navigation gaps persist in remote regions and NE India.

11.2 Measures Taken by Government of India for Airspace Management

Measure	Details
1. Flexible Use of Airspace (FUA) Policy – 2020	Allows real-time sharing of airspace between civil and military users. Improves fuel efficiency, reduces flight time, and aligns with ICAO norms. Implemented jointly by AAI and IAF.
2. Airspace Mapping and Rationalisation	Over 128 restricted airspace routes have been made available to civilian flights (as of 2023). Aligns with the PM Gati Shakti vision for efficient logistics and multi-modal connectivity.
3. No Permission No Takeoff (NPNT) Policy for Drones	Mandates all drones to be registered and permitted digitally before flying. Integrated with the Digital Sky Platform to prevent unauthorised UAV operations.
4. Digital Sky Platform (DGCA)	A cloud-based UAS Traffic Management (UTM) system for drone flights under controlled airspace. Categorises zones into *Green, Yellow,* and *Red,* streamlining low-altitude airspace regulation.
5. Deployment of RADARS and ADS-B Systems	Expansion of radar coverage, ADS-B (Automatic Dependent Surveillance – Broadcast) systems, and ground stations to reduce radar blind spots, especially in NE, island, and coastal zones.
6. Establishment of Air Defence Command (ADC)	Under proposed theatre commands, the ADC would unify all airspace-related military assets under one umbrella, ensuring faster response and coordinated surveillance.
7. Strengthening ADIZ and Border Air Defence Zones	IAF upgrading low-level radar networks, electro-optical sensors, and integrating civil ATC data to monitor aerial intrusions in border areas (*PoK, Ladakh, NE India*).
8. Integration with ICAO and Neighbouring FIRs	Coordination with ICAO and neighbouring Flight Information Regions for *seamless airspace corridors,*

	better detection, and smooth international overflight procedures.
9. Counter-Drone Technology Deployment	DRDO-developed anti-drone systems, RF jammers, and soft kill lasers deployed at critical airports, border areas, and strategic airfields to mitigate low-altitude threats.
10. Strengthening of UAV Command and Control Rules (2021)	Introduced *mandatory compliance with geo-fencing, return-to-home,* and *remote ID protocols,* aiming to align with global air traffic safety norms.

12. Impact of Civil–Military Collaboration in Improving Border Management in India

Area of Impact	Description
1. Enhanced Border Surveillance	*Civil–military synergy* integrates community vigilance with military surveillance systems. Local civilians act as eyes and ears, reporting suspicious activities along LoC and LAC, while forces like BSF and ITBP deploy force multipliers (such as thermal imagers). Real-time intelligence enables better cross-border monitoring and border integrity.
2. Infrastructure Development	Joint efforts between BRO and civil administration build strategic roads and all-weather connectivity. BRO's 2025 LAC roads counter China's salami slicing tactics and enable rapid troop mobilisation. Civilian buffers in border villages further support logistics and preparedness.
3. Community Engagement and Stability	Collaboration fosters trust through civic programs (*Sadbhaavana*, Vibrant Villages Programme), providing healthcare and jobs to reduce migration and discontent.
4. Counter-Insurgency Operations	Civilians provide local intelligence to forces, improving targeted operations against insurgents (e.g., Assam's civil administration sharing data on ULFA networks in Indo-Myanmar region).
5. Economic Integration	Border Haats along India–Bangladesh and India–Nepal borders reduce smuggling and FICN circulation, fostering cross-border synergy and economic stability.
6. Disaster Response and Resilience	Coordination enhances disaster management in border areas — e.g., *NDRF and ITBP with Arunachal civil administration during Brahmaputra floods (2024).*
7. Countering Illegal Activities	Gujarat's coastal communities work with Coast Guard
8. Diplomatic and Strategic Support	In 2024–2025, the Ministry of External Affairs and the Army collaborated on LAC negotiations with China, establishing civilian buffers in Depsang to counter incremental encroachments.
9. Capacity Building	In 2024, BSF trained J&K's VDCs in intelligence gathering, enabling locals to support smart border management. This civil–military synergy improved operational efficiency along the LoC.

10. Psychological Operations	Joint information campaigns by civil authorities and military counter-propaganda and radicalisation teams. In 2025, civil–military teams in J&K used social media to promote national unity, reducing separatist sentiments and reinforcing border community loyalty.

13. Border Management Initiatives by Government of India

Initiative	Description
1. Comprehensive Integrated Border Management System (CIBMS)	Deploys *smart border management* with force multipliers like **CCTV, thermal imagers, motion sensors, and drones** along *Indo-Pakistan* and *Indo-Bangladesh borders,* integrated with **AI-enhanced analytics in 2025** for real-time surveillance.
2. Smart Border Fencing	Installs *double-row fencing* with **laser barriers and anti-drone nets** along Line of Control (LoC), Radcliffe Line, and Indo-Bangladesh borders, incorporating **smart sensors** in **2024** to enhance border security.
3. Vibrant Villages Programme	Develops over **100 LAC villages** along Indo-China border as *civilian buffers* with roads, healthcare, and jobs, expanded in **2025** to counter *China's salami slicing tactics.*
4. Space-Based Surveillance	Utilises **NAVIC, Cartosat, and GSAT satellites** for real-time imagery of LAC and LoC hotspots, integrated with **AI-enhanced analytics in 2024** to monitor border activities.
5. Maritime Anti-Piracy Act, 2022	Enforces legal frameworks to *combat piracy along maritime borders*, prescribing life imprisonment or the death penalty, implemented in **2023** to protect trade routes.
6. Madhukar Gupta Committee Recommendations	Establishes a *border security grid* for coordinated response along the Indo-Pakistan border, **prioritising complete fencing and real-time monitoring** with *AI-based analytics* in **2025.**
7. Termination of Free Movement Regime (FMR)	Ends **FMR along the Indo–Myanmar border in 2024**, initiating fencing in **2025** to restrict *insurgent mobility* and *drug trafficking.*

Conclusion

India's border management, through a **Whole of Nation Approach**, leverages *civil–military synergy* and *smart technology* to ensure **strategic deterrence** and **economic growth.**
Robust security and community engagement foster a resilient nation, culminating in:
Surakshit Seemayen, Sashakt Bharat; Surakshit Seemayen, Samriddha Bharat.

Linkages of organized crime with terrorism

As per UNTOC - It is a *structured group* of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes, in order to obtain — directly or indirectly — a **financial or other material benefit (profits).**

1. Major Forms of Organized Crime in India

Type	Description & Relevance to India	Key Examples / Facts
Drug Trafficking	India lies between the **Golden Triangle (Myanmar–Laos–Thailand)** and **Golden Crescent (Iran–Afghanistan–Pakistan)**, making it a major transit and consumption hub. Leads to **narco-terrorism**, **social crimes**, and **corruption**.	Heroin, hashish, opium, methamphetamine smuggled across borders; terror networks in Punjab & J&K finance operations via drug money.
Arms Smuggling	Illegal trade of weapons, explosives, and advanced tech through porous borders.	Routes via Pakistan, Bangladesh & Myanmar.
Human Trafficking	Recruitment, transport, exploitation of people through coercion, fraud, or abduction. India acts as **source, destination & transit**.	High cases in Assam, WB, Tamil Nadu, Telangana.
Counterfeiting (FICN)	Fake Indian Currency Notes fund terrorism, especially in **Kashmir**.	Smuggled via Nepal, Bangladesh, Pakistan. **FICN Coordination Group (FCORD)** under MHA tackles issue.
Cybercrime	Hacking, cyber-attacks, financial frauds, and social engineering used for funding & destabilization.	Threatens national & economic security.
Extortion & Kidnapping for Ransom	Used by insurgents and terror groups to fund activities.	Common in **Northeast India**; ransom often directed to terror networks.

2. Characteristics of Organised Crime

Characteristic	Explanation
Organised (Hierarchical) Structure & Planning	Groups are highly structured and follow a clear chain of command; decisions and operations are planned meticulously.
Continuity	The organisation exists over a long period of time and sustains operations even after leadership changes.
Criminality	Engages repeatedly in serious crimes such as smuggling, trafficking, extortion, contract killings, cybercrime, etc.
Power / Profit Motive	The principal aim is to accumulate wealth and influence; power becomes an instrument for profit generation.
Secrecy & Restricted Membership	Membership is limited to trusted individuals; operations are hidden from law enforcement through coded communication and secrecy.
Violence, Intimidation & Threat	Violence is used to eliminate rivals, control territory, and intimidate witnesses.
Use of Corruption	Corruption of officials ensures protection, manipulation of law, and continuity of illegal business.

3. Organised Crime vs Terrorism

Aspect	Organised Crime	Terrorism
Nature	Profit-driven (economic) criminal groups.	Essentially political or ideological groups.
Motive	Driven by economic and financial objectives; aim to establish a **parallel economy.**	Driven by political or religious motives (fundamentalism); aim to **topple governments** (ISIS, Taliban, Al-Qaeda, Boko Haram).
Methods	Use violence to protect business interests; prefer secrecy to avoid public exposure.	Use large-scale violence and civilian killings to instil fear among target communities; seek **media attention** for propaganda.
Primary Goal	Financial gain and control over illegal markets (drug trade, arms, human trafficking).	Political change, religious dominance, or ideological enforcement.
Structure	Hierarchical with limited membership; motivated by profit.	Cell-based networks; motivated by ideology.
Relationship Overlap	May collaborate for mutual benefit — e.g., terrorists funding activities through smuggling or narcotics trafficking.	May depend on organised crime for logistics, weapons, or money laundering.

4. The Crime–Terror Nexus

"Terrorism is funded by laundering; Anti-money laundering is counter-terrorism." – *UN Security Council*

Mechanism	Explanation / Examples
Terrorist Financing	Terror groups create revenue through drugs, arms, and extortion. E.g. *Taliban's opium trade*; *Lashkar-e-Taiba* funds via NGOs, hawala.
Money Laundering as Lifeline	Laundered money sustains terror networks — used for weapons, camps, propaganda, and recruitment.
Punjab Case Study	*Golden Crescent + Pakistani cartels* fuel **Khalistani separatism**; heroin trade via drones from Pakistan.
Criminalized Insurgencies (UNODC)	*Myanmar's Arakan Army* earns 60% from meth trade; blurs political and profit motives.

5.Global Examples

Country/Group	Type of Linkage	Details
Taliban (Afghanistan)	*Drug-Terror Nexus*	Financed insurgency through opium cultivation and heroin trade.
ISIS (Iraq & Syria)	*Resource Smuggling*	Earned billions through oil smuggling, kidnapping, and looting of antiquities.
FARC (Colombia)	*Narco-Terrorism*	Transformed from Marxist rebels into cocaine traffickers funding insurgency.
Hezbollah (Lebanon)	*Money Laundering Networks*	Operates global fundraising through drug and currency laundering.
Boko Haram (Nigeria)	*Human Trafficking & Extortion*	Funds operations through kidnapping and illegal trade in conflict minerals.

6. Why the Linkage Matters

Effect	Explanation
Force Multiplier Effect	Organized crime and terrorism amplify each other's strength.
Escalation of Threats	Joint operations create larger, transnational danger.
Erosion of Sovereignty	Undermines economic and political stability; fuels corruption.
Global Nature	Requires international cooperation due to cross-border networks.

7. Crime–Terror Nexus in the Indian Context

Region	Key Issues	Details / Examples
Jammu & Kashmir	State-sponsored terror (ISI), foreign funding (Gulf), narco-terrorism (15% finances).	Drug trafficking sustains militant operations.
Punjab	Drug crisis due to proximity to Pakistan; heroin trade finances separatism; drones used for arms/drug smuggling.	Heroin routes from Pakistan; drone infiltration worsens security.
Northeast India	Golden Triangle hub; transnational networks; insurgent extortion.	Myanmar–Cambodia–Laos links; parallel "taxation" by insurgents.
Coastal Security	Smuggling of arms, narcotics, explosives; post-26/11 reforms.	Enhanced coastal surveillance & intelligence networks.
Cyber Domain	India = 2nd most cyber-attacked nation (2025); digital terror financing.	Drones, virtual assets, crypto used for recruitment & ops.

8.Impact of the Nexus

Dimension	Impact	Illustration
1. National Security	Increases terrorism, destabilises states, and erodes public trust in governance.	*Mumbai 1993 Blasts; Kashmir insurgency funding via Hawala.*
2. Economic Impact	Parallel black economy; diversion of funds from productive sectors.	*FICN circulation; narcotics trade; money laundering.*
3. Political Impact	Criminal-political nexus; loss of state legitimacy.	*Election funding through illegal networks.*
4. Social Impact	Erosion of law and order; youth radicalisation.	*Recruitment via drug mafia and local gangs.*
5. International Impact	Cross-border terrorism; diplomatic friction.	*India–Pakistan relations; FATF compliance issues.*

9.Indian Efforts to Counter the Nexus

Measure	Key Provisions / Actions	Example / Impact
Unlawful Activities (Prevention) Act (UAPA) 1967	Empowers government to ban organisations and seize properties involved in terror-financing or organised crime.	Used against Dawood Ibrahim network & PFI.
National Investigation Agency (NIA)	Central agency investigating terror financing and cross-border crimes.	*NIA–ED coordination in D-Company and ISIS cases.*

Prevention of Money Laundering Act (PMLA) 2002	Enables tracing and confiscation of proceeds of crime.	Used in *Hawala and terror-funding probes.*
Narcotic Drugs and Psychotropic Substances (NDPS) Act 1985	Controls narcotics trade which often funds terrorism.	*Crackdown on drug routes in Punjab & Manipur.*
FATF (Financial Action Task Force) Compliance	India participates globally to monitor illicit financial flows and pressure Pakistan to curb terror-financing.	*Pakistan retained under FATF Grey List until 2022.*
Strengthening Border Management	Fencing, surveillance drones, and integrated check posts (ICPs) to curb smuggling and infiltration.	*BSF & Coast Guard coastal radar network.*
Inter-Agency Coordination	Intelligence Bureau, ED, RAW, and NIA joint task forces.	*Multi-Agency Centre (MAC) sharing real-time intelligence.*

---

10. Way Forward

Strategy	Description
1. Financial Intelligence Strengthening	Enhance FIU-IND, ED, and RBI coordination to trace cross-border financial flows and block Hawala routes.
2. International Cooperation	Engage with INTERPOL, FATF, and UNODC to share real-time intelligence on transnational crimes.
3. Legal Reforms	Introduce a **Comprehensive Organised Crime Control Act** to address nexus beyond existing state-level MCOCA/TNOC Acts.
4. Technology Integration	Use blockchain analysis, AI surveillance, and forensic accounting to track illicit money movement.
5. Community Engagement	Involve local populations and civil society in counter-radicalisation and anti-drug programmes.
6. Capacity Building	Strengthen police and border agencies with cyber-forensics and financial investigation skills.
7. Regional Diplomacy	Collaborate with neighbours like Nepal, Bhutan, Bangladesh, and Myanmar to dismantle shared criminal-terror networks.

3.5 Various Security forces and agencies and their mandate

The Indian internal-security framework **comprises various security forces and agencies**, including the **Central Armed Police Forces (CAPFs)**, **intelligence agencies**, and **specialised units**.
Each has distinct mandates to tackle insurgency, terrorism, border security, and cyber threats. They function under the **Ministry of Home Affairs (MHA)** and collaborate to maintain law and order, safeguard sovereignty, and ensure stability.

---

1. Central Armed Police Forces (CAPFs)

Seven central police organisations under MHA, responsible for internal security and border guarding — **Assam Rifles (AR), Border Security Force (BSF), Central Industrial Security Force (CISF), Central Reserve Police Force (CRPF), Indo-Tibetan Border Police (ITBP), National Security Guard (NSG)** and **Sashastra Seema Bal (SSB)**.
They are **vital in maintaining law and order and protecting India's frontiers.**

1.1 Border Security Force (BSF)

Established 1 Dec 1965 – India's *primary border-guarding* and world's *largest border-security organisation.*

Aspect	Responsibilities
1. Peacetime Duties	Guarding borders; prevention of unauthorised entry/exit, smuggling, and infiltration; intelligence collection of trans-border activity. *Example:* In 2025, BSF seized 100 drones used by terror groups for smuggling arms and drugs into Punjab via Indo-Pak border.
2. Wartime Duties	Holding sectors, guiding Army in border areas, assisting refugee control, conducting special intelligence & cross-border raids, guarding POWs. *Example:* During 1971 Indo-Pak War, BSF battalions held key sectors in Rajasthan & Punjab.
3. Additional Roles	Assisting Army with local knowledge, performing internal-security duties on State Govt request, conducting counter-insurgency & counter-terror ops. *Example:* In 2025, BSF deployed five additional companies in Murshidabad to control violence during Waqf protests.

1.2 Indo-Tibetan Border Police (ITBP)

Established 1962 after the Sino-Indian War; motto **"Shaurya – Dridhata – Karm Nishtha"** (Valour, Steadfastness & Commitment).
Maintains security and prevents trans-border crime along the high-altitude Indo-China frontier.

Aspect	Responsibilities
1. Border Security	Patrols **3,488 km Indo-China border** with 32 battalions and 157 outposts up to 18,900 ft.
2. Disaster Response	First responder to Himalayan avalanches and landslides; 8 Regional Response Centres in Himachal, Uttarakhand & NE.
3. Special Skills & Achievements	Expertise in mountaineering, skiing & river rafting; multiple Republic Day trophies. *Example:* ITBP won Best Marching Contingent Trophy 1998, 1999, 2000, 2011.
4. COVID-19 Contributions	Quarantine camps & India's largest Covid Care Centre (New Delhi). *Example:* Managed 10,000-bed Sardar Patel Covid Centre in Chhatarpur for 12,000 patients.
5. Environmental Role	Greening & ecological conservation in remote Himalayan areas.
6. VVIP Security	Provided security to VVIPs – role may be withdrawn by MHA to focus on borders.

1.3 Sashastra Seema Bal (SSB)

Established 1963 after the Sino-Indian War; motto **"Service, Security and Brotherhood."**

Aspect	Responsibilities
1. Role	Prevents cross-border crime & anti-national activities along Indo-Nepal & Indo-Bhutan borders.
2. Legal Powers	Empowered under CrPC (1973), Arms Act (1959), NDPS Act (1985), Passport Act (1967); Customs Act (1962) powers proposed.
3. Area of Operation	Within 15 km belt along Indo-Nepal & Indo-Bhutan borders in Uttarakhand, UP, Bihar, WB, Sikkim, Assam & Arunachal Pradesh.

1.4 National Security Guard (NSG)

Established 1984 after Operation Blue Star & Indira Gandhi's assassination; elite counter-terror & hostage-rescue force.
Motto **"Sarvatra Sarvottam Suraksha" (Everywhere and Always the Best Security).**

Aspect	Responsibilities
1. Usage of NSG	For exceptional situations only – not for regular policing. *Example:* Deployed during 2008 Mumbai attacks.

2. Deployment in Kashmir	Since 2018 – supports counter-drone protection at IAF Srinagar & Jammu bases.
3. Role of NBDC	*National Bomb Data Centre* within NSG supports Post-Blast Investigations. *Example:* Analysis after 2013 Patna bombings.

1.5 Central Industrial Security Force (CISF)

Established 1969; protects industrial & critical infrastructure; motto **"Protection and Security."**

Aspect	Responsibilities
1. Critical Infrastructure Security	Security to nuclear installations, space establishments, airports, seaports & power plants. *Example:* Nuclear Power Plant Kudankulam.
2. Airport Security	Deployed since 2000 (post IC-814 hijacking); security at ~69 airports.
3. Protection of Govt Assets	Guards Parliament House, Delhi Metro, Red Fort, Central Jails.
4. VIP Security	Specialised round-the-clock VIP protection.
5. Fire Protection Services	Largest fire-protection service with dedicated customised wing.

1.6 Central Reserve Police Force (CRPF)

Established 1939 (renamed 1949); motto **"Service and Loyalty."**
India's premier central armed police force for internal security and law & order.

Aspect	Responsibilities
1. Crowd Control & Riot Control	Manages crowds/riots to maintain law and order. *Example:* Rapid Action Force (1992) for communal riots.
2. Insurgency Ops	Counter-insurgency vs militants incl. Left Wing Extremism. *Example:* Ops in J&K and NE.
3. Coordination of Security	Oversees election security in disturbed areas.
4. Protection of VIPs & Vital Installations	Security to key persons and critical infra.
5. Environmental Protection	Prevents degradation & protects flora/fauna in operational zones.
6. War-time Aggression Defence	Participates in defence duties. *Example:* 1962 Sino-Indian War (Hot Springs, Ladakh).
7. UN Peacekeeping	Contributes to UN missions globally.

8. Rescue & Relief Ops	Disaster response. *Example:* May 2025 – CRPF rescued 39 students in Kashmir Valley.
9. CoBRA	Specialised guerrilla unit for anti-Naxalite ops.

1.7 Assam Rifles (AR)

Oldest paramilitary force in India – motto **"Friends of the Hill People."**

Aspect	Responsibilities
1. Border Security	Guards Indo-Myanmar border; prevents infiltration & illegal activities.
2. Internal Security & Counter-Insurgency	Ops in NE & J&K.
3. Protection of Govt Structures	Secures vital installations in disturbed areas.
4. Disaster Relief & Humanitarian Aid	Provides aid during natural disasters.
5. Civic Action & Development	Community projects to foster trust & national integration.

2. Special Forces

2.1 Special Protection Group (SPG)

Established 1988 under Cabinet Secretariat to protect the Prime Minister and family.
Motto **"Sauryam Samarparam Surakshanam" – Bravery, Dedication, Security.**

Aspect	Responsibilities
1. Proximate Security to PM	Armed protection to PM at all times (domestic & abroad).
2. Protection of Immediate Family	Secures family residing at official residence.
3. Implementation of Security Measures	Manages ring round teams, cordons, access control, etc.
4. Coordination with State Govts & Agencies	Coordinates with states for PM's movement and security.

2.2 Indian Coast Guard (ICG)

Established Feb 1 1977 (commissioned Aug 19 1978); maritime safety arm of India.

Function	Description
1. Protection of Maritime Structures	Security of artificial islands, offshore installations & terminals.

2. Fishermen Safety	Safeguards fishermen and assists those in distress at sea.
3. Marine Environment Conservation	Prevents marine pollution.
4. Anti-Smuggling Support	Assists Customs in anti-smuggling ops.
5. Law Enforcement	Enforces laws within India's maritime zones.
6. Additional Duties	Ensures safety of life & property at sea and scientific data collection.

3. Intelligence Agencies

India's security architecture includes RAW, IB, NIA, NCCC and other specialised organisations under MHA and MoD addressing terrorism, insurgency, cybercrime and border protection.

3.1 Intelligence Bureau (IB)

Established 1887; world's oldest intelligence agency. Motto **"Always Alert."**

Functions	Description
1. Domestic Intelligence	Monitors human activities & security threats (per 1951 Himmatsinh Ji Committee).
2. Counter-Intelligence & Counter-Terrorism	Executes ops against espionage & terrorism. *Example:* IB intelligence in J&K & NE to prevent infiltration.
3. Intelligence Sharing	Coordinates with other agencies & police.
4. Security Clearances	Grants clearances to diplomats & judges before oath.
5. Wiretapping & Surveillance	Intercepts communications to monitor threats (Indian Telegraph Act).
6. Advisory Role	Advises state & central govts on security matters.
7. Confidential Ops	Operates under high secrecy with no public disclosure.

3.2 Research and Analysis Wing (R&AW)

Established 1968 under PMO; India's foreign intelligence agency.
Motto **"Dharmo Rakshati Rakshitah."**

Functions	Description
Monitoring Political, Military, Economic, Scientific Developments	Tracks foreign developments impacting India's security.
Moulding International Public Opinion	Engages in covert diplomacy and influence ops.

Covert Operations	Secret missions to protect national interests. *Example:* Operation Smiling Buddha (1974).
Anti-Terror Operations	Identifies & neutralises terror threats abroad. *Example:* RAW busted ISI spy ring (Delhi, 2025).

3.3 National Investigation Agency (NIA)

Established 2008 under NIA Act; India's premier counter-terror law-enforcement agency. Motto **"Nation's Protection is the First Duty."**

Aspect	Responsibilities
1. Investigate Scheduled Offences	Under UAPA, Arms Act, Explosives Act, etc.
2. Initiate on Central Orders	May take up cases anywhere in India without state permission.
3. Prosecute in Special NIA Courts	For speedy trial & adjudication.
4. Coordinate with State Police	Ensures effective investigation & law enforcement in terror cases.
5. Conduct Extraterritorial Ops	Empowered by NIA (Amendment) Act

3.4 Mandates of Other Key Indian Intelligence and Security Agencies

Agency	Mandate
1. National Technical Research Organisation (NTRO)	• **Established in 2004** under the Prime Minister's Office and National Security Advisor, NTRO specializes in **technical intelligence** gathering through *satellite imagery, signal interception, cyber intelligence,* and *cryptology* to support internal and external security. • It provides **high-tech surveillance**, **monitors critical infrastructure**, and **aids other intelligence agencies** with advanced technical inputs.
2. Directorate of Revenue Intelligence (DRI)	• The DRI is the apex **anti-smuggling intelligence and enforcement agency** under the Ministry of Finance, **tasked with curbing smuggling, economic offenses, and customs fraud.** • It **collects intelligence on illicit trade**, monitors **cross-border movement of contraband**, and **enforces laws** related to customs and narcotics to protect India's economic security.

3. National Cyber Coordination Centre (NCCC)	• NCCC **functions as a central hub for cyber-threat monitoring** and coordination across various government agencies. • It **detects, analyses, and responds to cyberattacks** targeting critical information infrastructure, **ensuring cybersecurity and resilience of government networks and services.**
4. Joint Cipher Bureau (JCB)	• JCB is **responsible for cryptologic and signal intelligence operations**, providing **secure communication and encryption** support to Indian intelligence and security agencies. • It **plays a key role in intercepting and decoding foreign communications** to safeguard national security.
5. Multi-Agency Centre (MAC)	• MAC **serves as the nodal point for intelligence sharing and coordination** among various central and state agencies to **combat terrorism and insurgency.** • It **facilitates real-time information exchange, threat assessment, and joint operational planning** to **strengthen India's internal security framework.**
6. National Security Council (NSC)	• The NSC is the **apex body for strategic decision-making on national security and foreign policy.** • It **formulates policies, coordinates** among intelligence and security agencies, and **advises the Prime Minister** on internal and external security threats, **ensuring a comprehensive approach to safeguarding India's sovereignty and integrity.**

Operation Sindoor

Operation Sindoor, launched on **May 7 2025**, marks a **pivotal moment in India's counter-terrorism strategy**, triggered by the **Pahalgam terror attack** on **April 22 2025**, which killed 26 civilians (25 Indians and one Nepali tourist).

Operation executed by the **Indian Armed Forces** targeted **nine terrorist infrastructure sites** in **Pakistan** and **Pakistan-occupied Jammu and Kashmir (PoJK)**, focusing on groups like **Lashkar-e-Taiba (LeT)**, **Jaish-e-Mohammed (JeM)**, and **Hizbul Mujahideen (HuM)**.
It was described as a **focused, measured, and non-escalatory** operation; it avoided Pakistani military installations, **emphasising strategic restraint**.
It was the **most precise and successful operation in the history of India's response to terrorist attacks on its soil**, fulfilling all its objectives.

1. Background of Operation Sindoor

Aspect	Details
1. Pahalgam Terror Attack	• On April 22 2025, *The Resistance Front (TRF)*, an offshoot of *Lashkar-e-Taiba (LeT)*, executed a brutal attack in Baisaran meadow of Pahalgam, J&K, killing 26 tourists after segregating them by religion. • TRF claimed responsibility twice, with India linking the group to Pakistan-based LeT, highlighting the need for decisive action.
2. Pakistan's Role	• Pakistan's persistent refusal to dismantle terror networks like LeT and JeM, despite India's evidence from past attacks (e.g. Mumbai 2008, Pulwama 2019), necessitated a response. • India submitted a dossier to the **UN 1267 Sanctions Committee** documenting Pakistan's complicity in sheltering terrorists, underscoring its role in state-sponsored terrorism.
3. Historical Context	• India's prior **surgical strikes in 2016 (Uri)** and **2019 (Balakot)** targeted terror infrastructure in Pakistan/PoJK, but the operation was broader, **hitting nine sites across multiple groups like LeT, JeM, and HuM**, building on the precedent of proactive counter-terrorism.
4. Geopolitical Tensions	• Rising Indo-Pak tensions, marked by **diplomatic expulsions** and Pakistan's threat to suspend the Simla Agreement, created a volatile backdrop. • India's **suspension of the Indus Waters Treaty** post-attack was a strategic response to Pakistan's inaction against terrorism.

Various Operations Done by India on Pakistani Soil

Operation	Year	Details
Operation Trident	1971	Naval attack on Karachi port during the Indo-Pak War.
Operation Python	1971	Follow-up naval strike on Karachi port.
Operation Talwar	1999	Naval blockade of Karachi during the Kargil War.
Myanmar Counter-Insurgency	2016	Surgical strike on NSCN-K militants in Myanmar, contextually relevant near Pakistan border.
Operation Sindoor	2025	Precision strikes on nine terror sites in Pakistan/PoJK post-Pahalgam attack.
Operation Bandar	2019	Airstrike on JeM camp in Balakot, Pakistan, post-Pulwama attack.
Uri Surgical Strike	2016	Surgical strike on NSCN-K militants in Myanmar contextually relevant near Pakistan border.

2. Details of Operation Sindoor

Aspect	Details and Context
1. Date and Scope	Launched on **May 7 2025**, the operation targeted nine terror sites — **four in Pakistan** (such as Markaz Taiba, Muridke – LeT; Markaz Subhan

	Allah, Bahawalpur – JeM)** and **five in PoJK** (such as Syedna Bilal Camp, Muzaffarabad – JeM)** aiming to dismantle terrorist infrastructure linked to the Pahalgam attack.
2. Forces Involved	A coordinated effort by the **Indian Army, Navy, and Air Force**, utilising Rafale jets equipped with **SCALP missiles, HAMMER bombs, and loitering munitions**, showcasing tri-service synergy and advanced weaponry.
3. Weapons Used	• Employed a mix of indigenous (**Akash, BrahMos, NavIC-guided munitions**) and imported systems (**SCALP, HAMMER**). • **Akash** neutralised Pakistani drones; **BrahMos** ensured sub-meter precision, highlighting India's technological edge.
4. Execution	The **23-minute operation**, conducted from Indian territory, avoided Pakistani military installations to maintain a **non-escalatory strategy**, with strikes targeting specific buildings to minimise collateral damage.
5. Pakistan's Response	Pakistan escalated on May 8 with drone and missile strikes on Indian cities (e.g. Srinagar, Patiala), **neutralised by S-400 and Akash systems**; India retaliated on May 10, targeting military air bases like Rafiq and Bannu.
6. Outcome	Destroyed terror networks, killed over 100 terrorists, and neutralised hostile assets like Pakistan's **PL-15 missiles and Chinese-origin drones** without Indian losses, showcasing operational success.

Defence Systems Used by India During Operation Sindoor

System	Details
Akash Missile System	Indigenous short-range SAM; neutralised drones/missiles; multi-target engagement; ECM-resistant.
BrahMos Missile	Supersonic cruise missile; struck terror camps (such as Muridke) in 23-minute ops.
S-400 System	Russian long-range SAM; intercepted high-speed missiles/drones; protected Punjab/J&K installations.
SCALP Cruise Missile	Air-launched, long-range, precision strikes on terror sites (such as Bahawalpur) via Rafale jets.
HAMMER Munition	French guided bomb (GPS/laser); hit mobile/concealed targets (such as Muzaffarabad camps).
Loitering Munitions	Kamikaze drones; real-time surveillance & strikes (such as Rahim Yar Khan radar).
NavIC Navigation	Indigenous sub-meter precision targeting for BrahMos; paired with Cartosat/RISAT for 24×7 surveillance.
Rajendra Radar	Indigenous tracked radar; integrated with Akash/S-400 for air defence.
Akashteer	C&C system linking sensors/radars/missiles (Akash, S-400) for real-time response to threats.

3. Need for Operation Sindoor

Aspect	Details
1. Counter-Terrorism	Operation was **critical to neutralise Pakistan-based terror groups** (LeT, JeM, HuM) responsible for the Pahalgam attack that killed 26 civilians, with TRF (linked to LeT's Muridke camp) claiming responsibility — underscoring the **urgency to disrupt terror networks**.
2. National Security	Protecting India's sovereignty and civilian lives from cross-border terrorism was paramount as the Pahalgam attack exposed vulnerabilities in J&K's security grid, necessitating a robust response to **safeguard national interests**.
3. Deterrence	Operation Sindoor aimed to **deter state-sponsored terrorism** and counter Pakistan's nuclear blackmail, building on India's post-Pulwama (2019) resolve to **respond decisively to terror provocations**.
4. Pakistan's Inaction	Pakistan's refusal to act against terror groups, despite India's evidence from attacks like Mumbai 2008 and Pathankot 2016, and its stalling of joint probes, left India with no option but direct action to ensure accountability.

4. Significance of Operation Sindoor

Aspect	Details
1. New Security Doctrine	Established a bold doctrine **rejecting nuclear blackmail**, targeting both terrorists and their masterminds, with strikes on LeT and JeM camps signalling that India will not negotiate with terror sponsors, **redefining its counter-terrorism approach**.
2. Technological Prowess	Showcased **Aatmanirbhar Bharat** through indigenous systems like Akash, NavIC, and BrahMos. Neutralising PL-15 missiles and Chinese-origin drones in a 23-minute operation proved India's technological superiority.
3. Diplomatic Leverage	The **suspension of the Indus Waters Treaty**, linked to Pakistan's terror policy, enhanced India's strategic pressure, with the treaty's abeyance cited as a response to **Pakistan's violation of goodwill**.
4. Global Messaging	Demonstrated **strategic restraint** by avoiding military targets and debunking Pakistan's false claims (such as S-400 destruction), reinforcing India's adherence to international norms and countering propaganda.
5. Regional Stability	Redefined India-Pakistan engagement rules with a **zero-tolerance stance on terrorism**, with May 10 strikes on Pakistani air bases piercing Rawalpindi's perceived invincibility, fostering a new strategic equilibrium.
6. Diplomatic Realignment	Reduced engagement with Pakistan's allies like **Turkey and Azerbaijan** (by revoking Turkish Celebi's airport clearance) while **strengthening ties with Japan and Vietnam** to bolster counter-terror alliances.

5. Future Course of Action

Aspect	Details
1. Strengthen Intelligence	Enhance IB, RAW & state police intelligence integration. **20-minute response delay** exposed critical gaps — ensure **proactive threat detection**.
2. Restore J&K Statehood	Expedite J&K statehood restoration to win local support and curb terror logistics, as 15 locals aided Pahalgam attackers. Statehood promised to address alienation.
3. Expand Drone Capabilities	Develop indigenous **drone swarms and counter-UAS systems** to combat Pakistan's drone warfare (as seen May 8-9 swarms) and **maintain technological edge**.
4. Upgrade Air Force	Increase IAF squadrons to 42 and fast-track the AMCA project to counter Pakistan and China, addressing the current 31-squadron deficit while noting **China's J-20 advancements**.
5. Target Terror Leaders	Pursue high-value targets in Pakistan through covert operations or strikes as notorious LeT and JeM leaders remain active, requiring **sustained counter-terror efforts**.
6. Global Advocacy	Push for UN sanctions on TRF and Pakistan's return to the **FATF Grey List**, with India's post-Pahalgam lobbying at the UN to strengthen **global counter-terrorism measures**.
7. Non-Military Pressure	Leverage **Indus Waters Treaty suspension** and economic measures to deter Pakistan's terror support, using the treaty as a strategic tool for non-military coercion.

Conclusion

Operation Sindoor was a **decisive military operation** targeting terror infrastructure in Pakistan, marking a **new chapter in India's fight against terrorism**. It set a new benchmark and established a firm stance — terrorism will not be tolerated.
As Prime Minister Modi stated:

"This is not an era of war, but it is not an era of terrorism either."

CHANAKYA IAS ACADEMY
Nurturing Leaders of Tomorrow
SINCE 1993

CIVILS WITH AKASH

WAY FORWARD TEMPLATE FOR INTERNAL SECURITY

Mnemonic: SECURITY (Strengthening-Empowerment-Coordination-Upgradation-Resources-Intelligence-Technology-Youth)

HEADING	SUB-HEADING	POINT	DATA & EXAMPLES
STRENGTHENING INSTITUTIONS	Legal Framework	New laws, Fast-track courts, Conviction improvement	NIA conviction 94.7% vs state 32%; Need UAPA amendments; 312 pending cases
	Agency Capacity	Manpower, Training, Specialization	CAPF 78,000 vacancies; Only 15% trained in CBRN; Add 50,000 personnel
	Accountability	Oversight mechanisms, Human rights compliance	1,800 custodial deaths (2020-24); Need independent oversight body
EMPOWERMENT	Local Communities	Village defense committees, Community policing	4,500 VDGs in J&K; Mizoram community policing reduced crime 23%
	Gram Sabhas	PESA implementation, Local governance in tribal areas	Only 4/10 states implement PESA; Empower 2.5 lakh gram sabhas
	Civil Society	NGO partnership, Rehabilitation programs	67% Naxal surrenders through NGO counseling; Scale up surrender policy
COORDINATION	Inter-Agency	NATGRID completion, Unified command	NATGRID 40% operational; Complete by 2025; Need NCTC revival
	Center-State	Real-time intel sharing, Joint operations	MAC prevented 47 attacks; Expand SMACs to 300 cities from 200

	International	MLA treaties, Extradition, Intelligence sharing	204 MLA pending; Fast-track with 20 priority countries
UPGRADATION	Equipment	Modern weapons, Protective gear, Vehicles	50,000 BPJ shortage; 68% weapons outdated; ₹15,000 crore modernization
	Infrastructure	Barracks, Medical facilities, Communication	40% barracks dilapidated; Build 500 new facilities; 5G for forces
	Forces Welfare	PTSD counseling, Leave policy, Family support	300 CAPF suicides annually; Mandatory counseling; Reduce 14-hr duty
RESOURCES	Development	Roads, Schools, Hospitals in LWE/border areas	5,422 km roads in LWE; Complete 3,800 km pending; 4,072 mobile towers
	Employment	Skill centers, Job creation in vulnerable areas	17.3% youth unemployment; Open 100 ITIs in LWE districts
	Financial Inclusion	Banking, Insurance, Pension in remote areas	Only 54% accounts active in LWE; Expand Jan Dhan by 2 crore
INTELLIGENCE	HUMINT	Ground intelligence, Informer networks	Heavy tech reliance; Revive informer networks with protection
	Technology Integration	AI for predictive analysis, Data mining	Predictive policing reduced Mumbai crime 18%; Expand to 50 cities
	Cyber Intelligence	Dark web monitoring, Crypto tracking	847 dark web arrests; Set up Cyber Forensic Labs in all states
TECHNOLOGY	Border Management	CIBMS completion, Drone surveillance, Smart fencing	₹9,763 crore CIBMS; Complete 10 pilots by 2026; 1,000 more drones
	Cybersecurity	Critical infrastructure protection, SOC setup	67 infra attacks (2023); 24x7 SOC for power, banking, railways

	Communication	Interoperable systems, Encrypted channels	Different wireless systems; Single secure communication network
YOUTH ENGAGEMENT	Education	Quality schools, Digital access, Scholarships	68% LWE dropout; Open 500 Eklavya schools; Free internet
	Skill Development	Vocational training, Entrepreneurship support	Only 15% skilled in LWE; Train 10 lakh youth; ₹5,000 crore fund
	Deradicalization	Counseling, Rehabilitation, Reintegration	122 ISIS arrests; Set up 20 deradicalization centers; Witness protection

QUESTION 1

"Left-wing extremism continues to pose a significant challenge to India's internal security despite declining incidents. Critically examine the socio-economic factors responsible for the persistence of Naxalism and suggest a comprehensive roadmap for its resolution." (250 words, 15 marks)

ANSWER 1

INTRODUCTION

Left-wing extremism, affecting 90 districts across 11 states with 223 deaths in 2025, persists despite geographical shrinkage from 106 districts in 2018. The movement's resilience stems from deep-rooted socio-economic grievances in tribal heartlands rather than ideological appeal alone, demanding development-centric rather than purely security-driven solutions.

BODY: SOCIO-ECONOMIC FACTORS

Using Template 1: DEPRIVED (Development-Economic-Political-Resource-Institutional-Vulnerability-Education-Displacement)

D - DEVELOPMENT DEFICIT	Challenge	Examples/Data
Backwardness	Regional disparity, Infrastructure gap	90% LWE districts in Scheduled Areas; Bastar literacy 55% vs national 77.7%
Basic Services	Health, Education, Connectivity	45% areas have no secondary school within 5 km; Doctor ratio 1:5000 vs 1:1400 national

E - ECONOMIC DEPRIVATION	Challenge	Examples/Data
Poverty & Unemployment	Lack of livelihood, Income inequality	45% below poverty line vs 21% national; Per capita ₹48,000 vs ₹1,72,000
Land Alienation	Tribal land grabbed, Displacement	40% displaced are tribals; 2.5 million hectares transferred to non-tribals (1950-2020)

P - POLITICAL MARGINALIZATION	Challenge	Examples/Data
Governance Vacuum	Absent administration, No representation	Only 8% Panchayats functional in core Naxal areas (Chhattisgarh)
Voice Deficit	No participation, Ignored grievances	PESA implemented in only 4 of 10 scheduled states; Gram Sabhas powerless

R - RESOURCE EXPLOITATION	Challenge	Examples/Data
Mining & Forests	MNCs extracting, Locals not benefiting	80% coal, 60% bauxite in tribal areas; only 2-3% locals employed
Environmental Damage	Deforestation, Pollution	1.5 million hectares forest cover lost in mining areas (2015-2024)

I - INSTITUTIONAL FAILURE	Challenge	Examples/Data
Corruption	Siphoning of funds, Fake beneficiaries	₹50,000 crore leaked from MGNREGA in LWE states (CAG 2023)
Law & Order Collapse	Police brutality, Fake encounters	1,800+ custodial deaths in LWE states (2020-2024) - NHRC data

V - VULNERABILITY EXPLOITATION	Challenge	Examples/Data
Identity Crisis	Tribal culture threatened, Forced mainstreaming	573 tribal languages endangered; 12 extinct since 2000
Social Stratification	Caste discrimination, Class divide	SC/ST comprise 70% of Maoist cadre base

E - EDUCATION GAP	Challenge	Examples/Data

School Dropout	No schools, Poor quality	68% secondary dropout in LWE districts vs 36% national
Skill Deficit	No vocational training, Youth unemployable	Only 15% youth in LWE areas have skill training

D - DISPLACEMENT	Challenge	Examples/Data
Development Projects	Dams, Industries, Mining	60 million displaced since 1947; 40% tribals; 70% never rehabilitated
Rehabilitation Failure	No land for land, Cash compensation useless	Only 30% displaced received promised rehabilitation (2024 survey)

WAY FORWARD

SECURITY

TEMPLATE	HEADING	SUB-HEADING	SPECIFIC ACTIONS
SECURITY	**S - Strengthening**	Institutions, Legal	Fast-track 312 NIA cases; Independent Police Complaints Authority; End Salwa Judum-style operations
SECURITY	**E - Empowerment**	Gram Sabhas, PESA	Implement PESA in all 10 states with 2025 deadline; Empower 2.5 lakh Gram Sabhas with land veto
SECURITY	**C - Coordination**	Inter-agency, Center-State	Complete NATGRID by Dec 2025; MAC prevented 47 attacks—expand SMACs to 300 cities from 200
SECURITY	**U - Upgradation**	Equipment, Infrastructure	₹15,000 crore for 50,000 BPJ, modern weapons; Rebuild 40% dilapidated barracks; 5G connectivity
SECURITY	**R - Resources**	Development in LWE	Complete 3,800 km pending roads by 2026; Open 100 ITIs; ₹5,000 crore skill development fund
SECURITY	**I - Intelligence**	HUMINT, Technology	AI-powered predictive analysis in 50 cities; Cyber monitoring of Maoist sympathizers; Informer protection
SECURITY	**T - Technology**	Surveillance, Communication	Interoperable wireless for all forces; Satellite phones in zero-network areas; Drone fleet expansion
SECURITY	**Y - Youth Engagement**	Education, Employment	Open 500 Eklavya Model Schools; Train 10 lakh tribal

			youth; Corporate employment quotas (10% locals)

CONCLUSION

Integrated SAMADHAN-SECURITY approach combining development, technology, governance can sustainably resolve LWE.

QUESTION 2

"The changing nature of terrorism in India, with increased role of external state and non-state actors, demands a multi-pronged security response. Analyze the contemporary challenges and evaluate India's counter-terrorism strategy." (250 words, 15 marks)

ANSWER 2

INTRODUCTION

Indian terrorism has evolved from Kashmir-centric to hybrid threats—Pakistan-sponsored infiltration (47 attempts in 2024), ISIS radicalization (122 arrests 2020-24), Chinese cyber warfare (67 infrastructure attacks), and social media weaponization (4.2 million fake accounts removed). This multi-domain challenge demands comprehensive intelligence-led, technology-enabled counter-terrorism architecture beyond conventional kinetic operations.

BODY: CONTEMPORARY CHALLENGES

Using Template 2: PARTNERS (Pakistan-Adversaries-Radicalization-Terror-Networks-Espionage-Regional-Social Media)

P - PAKISTAN-SPONSORED TERRORISM	Challenge	Examples/Data
Terror Groups	LeT, JeM, HM operations	127 training camps in PoK; 308 ceasefire violations; 47 infiltration attempts (2024)
ISI Activities	Training, Funding, Handlers	Pulwama (2019): 40 CRPF martyred; Poonch (2024): Army convoy ambush

A - ADVERSARIES (STATES)	Challenge	Examples/Data
China	PLA incursions, Strategic encirclement	18 face-offs along LAC (2024); Galwan (2020): 20 soldiers martyred
Bangladesh	Border issues, Illegal immigration	4,096 km porous border; 20 million illegal immigrants; 40,000+ Rohingyas

R - RADICALIZATION	Challenge	Examples/Data
Islamic Extremism	ISIS, Al-Qaeda modules	122 ISIS-inspired arrests (2020-24); Kerala, Karnataka, UP modules
Wahhabism Spread	Saudi funding, Madrasas	24,010 unregistered madrasas; ₹2,400 crore foreign funding annually

T - TERROR ORGANIZATIONS	Challenge	Examples/Data
Active Groups	LeT, JeM, NDFB, ULFA	106 banned organizations under UAPA; 180 local youth joined militancy (2023)
Foreign Links	Pakistan, China, Myanmar bases	NSCN(IM) camps in Myanmar; ULFA in Bangladesh; Hybrid terrorists in J&K

N - NETWORKS	Challenge	Examples/Data
Sleeper Cells	Urban modules, Cyber cells	17 modules busted in Delhi, Mumbai, Hyderabad (2023-24)
Hawala Channels	Money routing, Gold smuggling	₹15,000 crore annual hawala; ₹8,000 crore gold smuggling from UAE

E - ESPIONAGE	Challenge	Examples/Data
Intelligence Ops	Honey trapping, Data theft	156 espionage cases (2020-24); Defence personnel targeted on dating apps
Cyber Espionage	State-sponsored hacking, APT groups	67 cyber attacks by China's APT groups (2023); Mumbai power grid suspected

R - REGIONAL CONFLICTS	Challenge	Examples/Data
Nepal Maoists	Cross-border shelter, Arms supply	4 camps along India-Nepal border (Uttarakhand, UP, Bihar)
Myanmar Insurgents	NSCN(K), ULFA camps	62 insurgent camps in Sagaing region; Arms smuggling via Moreh (Manipur)

S - SOCIAL MEDIA WARFARE	Challenge	Examples/Data
Propaganda	Fake news, Deepfakes, Misinformation	4.2 million fake accounts removed by MHA (2023); CAA, farmers' protest manipulation
Recruitment	Online radicalization, Encrypted apps	78% ISIS recruits contacted via Telegram/Facebook; Encrypted training calls

EVALUATION OF INDIA'S STRATEGY

POSITIVE MEASURES	Examples/Data
NIA Effectiveness	1,876 cases; 94.7% conviction vs state 32%; 312 ongoing cases
Op All Out	380 terrorists neutralized (2020-24); Attacks down from 417 (2018) to 67 (2023)
Legal Framework	UAPA amendments; PFI banned (₹120 crore seized); 22 designated NIA courts
Intelligence	MAC prevented 47 attacks (2020-24); SMACs in 200 cities
GAPS/LIMITATIONS	**Issues**
Slow Justice	312 NIA cases pending; Trials take 5-7 years; Witnesses turn hostile
No Unified Command	26/11 showed NSG-Police-Navy confusion; NCTC shelved due to state opposition
Reactive Approach	Post-attack response, not preventive; Limited HUMINT; Heavy tech reliance
No Deradicalization	Arrested youth not rehabilitated; Prisons become radicalization centers

WAY FORWARD

TEMPLATE	HEADING	SUB-HEADING	SPECIFIC ACTIONS
SECURITY	**S - Strengthening**	NIA, Legal Framework	Add 2,500 NIA officers; NIA branches in all 28 states; Financial investigation powers to NIA
SECURITY	**E - Empowerment**	Civil Society, NGOs	NGO partnerships: 67% Naxal surrenders via counseling—scale up for J&K; Community-based counter-radicalization
SECURITY	**C - Coordination**	NATGRID, NCTC, MAC	Complete NATGRID by Dec 2025 (currently 40%); Revive NCTC with state consensus; Expand SMACs to 300 cities
SECURITY	**U - Upgradation**	Equipment, Infrastructure	Anti-drone systems along Pakistan border; Modern weapons for 68% outdated arsenal; Secure communication
SECURITY	**R - Resources**	Border Infrastructure	₹10,000 crore for smart fencing completion; CIBMS 10 pilots by 2026; Satellite surveillance

SECURITY	**I - Intelligence**	HUMINT, TECHINT, Analysis	AI predictive policing in 50 cities; Dark web 24x7 monitoring; Joint interrogation centers (JICs)
SECURITY	**T - Technology**	Surveillance, Cyber Defense	Facial recognition at all airports, railway stations; Crypto transaction tracking; Social media analytics
SECURITY	**Y - Youth**	Deradicalization, Education	Track recidivism of 122 released; Engage families in rehabilitation; Scholarship programs for vulnerable youth

---

CONCLUSION

Multi-layered counter-terrorism combining prevention, detection, disruption, prosecution, deradicalization ensures comprehensive response.

QUESTION 3

"Cybersecurity has emerged as a critical dimension of national security with attacks on critical infrastructure and financial systems. Examine the vulnerabilities in India's cyber ecosystem and suggest measures for robust cyber defense." (250 words, 15 marks)

ANSWER 3

INTRODUCTION

India recorded 6.5 lakh cybercrimes (167% increase from 2019) with ₹1.25 lakh crore losses, making it the second-most targeted nation. AIIMS ransomware attack (6-week shutdown, 40 million records compromised) and Mumbai power grid suspected Chinese malware exemplify evolving cyber warfare threatening national security beyond kinetic domains.

BODY: VULNERABILITIES

Using Template 3: CRIMINAL (Cyber-Ransomware-Identity-Money-Infrastructure-Networks-Assistance-Laws)

C - CYBER THREATS	Challenge	Examples/Data
Critical Infrastructure	Power grids, Railways, Airports, Hospitals	67 attacks on critical infra (2023); Mumbai blackout (Oct 2020) Chinese malware suspected
Data Breaches	Personal info, Financial data leaks	75 million records leaked: Air India, IRCTC, BigBasket, Domino's

R - RANSOMWARE	Challenge	Examples/Data
Attacks	WannaCry, Maze, REvil variants	AIIMS (Nov 2022): 6 weeks shutdown, 40M records, ₹200 crore demand
Crypto Payments	Bitcoin demands, Untraceable	₹640 crore ransom paid by Indian entities (2020-23); Only 28% get data back

I - IDENTITY CRIMES	Challenge	Examples/Data
Aadhaar Leaks	Database breaches, Ghost entries	210 million Aadhaar details on dark web (₹5-50 per record)
Phishing	Banking frauds, OTP scams	₹1.25 lakh crore lost; 94,000 complaints daily; Deepfake CEO: ₹175 crore stolen

M - MONEY LAUNDERING	Challenge	Examples/Data
Hawala	Informal transfer, Terror funding	₹15,000-18,000 crore annual hawala; Dubai-Karachi-Kashmir route
Shell Companies	Benami properties, Black money	3.09 lakh shell companies struck off (2017-23); New ones emerge

I - INFRASTRUCTURE	Challenge	Examples/Data
Weak Systems	Outdated software, Unpatched vulnerabilities	68% govt websites vulnerable (CERT-In); 43% run unsupported Windows 7
IoT Vulnerabilities	Smart devices, SCADA systems	23 million IoT devices; 89% unprotected; Mirai botnet can weaponize

N - NETWORKS	Challenge	Examples/Data
Dark Web	Illegal marketplaces, Drugs, Arms, Data	847 Indians arrested (2020-24); 1,203 POCSO dark web cases
Cryptocurrency	Untraceable transactions, Terror funding	₹44,700 crore suspicious transactions; WazirX hack ₹2,000+ crore (North Korean Lazarus)

A - ASSISTANCE (International)	Challenge	Examples/Data
MLA Treaties	Mutual Legal Assistance, Extradition	204 MLA requests pending; 2-3 years average response time
Interpol Coordination	Red Corner Notices, Intelligence sharing	1,847 RCN against Indians; Countries refuse (asylum claims)

L - LEGAL FRAMEWORK	Challenge	Examples/Data
IT Act 2000	Sections 66, 67, 69, 70	52,974 cases (2023); Only 3.7% conviction rate; Trials drag 3-5 years
PMLA 2002	Money laundering prevention	5,422 cases; ₹9,870 crore attached; Only 23 convictions (0.4% rate)

WAY FORWARD

UsingTemplates: (SHIELD)

TEMPLATE	HEADING	SUB-HEADING	SPECIFIC ACTIONS
SHIELD	**S - Systems Protection**	Critical Infrastructure	Setup 24x7 SOCs for power, banking, railways; Air-gap SCADA systems; Quarterly penetration testing
SHIELD	**H - Human Capacity**	Training, Awareness	Train 10,000 cyber forensic experts; Cyber law for 5,000 judges; Cyber cells in all 16,000 police stations
SHIELD	**I - Information Security**	Data Protection, Encryption	Implement DPDP Act 2023 strictly; 100% data encryption; Mandatory 6-hour breach reporting (₹25 crore penalty)
SHIELD	**E - Economic Security**	Financial Systems, Banking	Real-time fraud detection using AI; Multi-factor authentication mandatory; Blockchain for transactions
SHIELD	**L - Legal Framework**	Laws, Courts, Prosecution	Fast-track cyber courts in all 28 states; Increase IT Act penalties 10x; Witness protection in cyber cases
SHIELD	**D - Defense Mechanisms**	Technology, Response	AI threat detection; Quantum encryption for defense; Incident response teams in all ministries

CONCLUSION

Layered cyber defense combining technology, legal reforms, capacity, international cooperation ensures resilience.

QUESTION 4

"Border management in India faces multifaceted challenges ranging from infiltration to organized crime networks. Critically analyze the issues in border security and evaluate the effectiveness of technological solutions like CIBMS." (250 words, 15 marks)

ANSWER 4

INTRODUCTION

India's 15,106 km land borders present diverse challenges—Bangladesh's riverine 4,096 km enables cattle smuggling (₹5,000-8,000 crore annually), Pakistan's 3,380 km witnesses 308 violations, China's 3,488 km LAC sees 18 face-offs (2024). With 47 infiltrations, ₹72,000 crore drugs seized, 67% terror funding from narcotics, borders remain vulnerable despite ₹9,763 crore CIBMS investment.

BODY: BORDER CHALLENGES

Using Template 4: BORDERS (Bangladesh-Operations-Regional tensions-Drugs-Espionage-Routes-Smuggling)

B - BANGLADESH BORDER	**Challenge**	**Examples/Data**
Illegal Immigration	Rohingya influx, Demographic change	20 million illegal immigrants; 40,000+ Rohingyas in camps
Cattle Smuggling	₹5,000-8,000 crore annually	2.5 lakh cattle smuggled; Only 81% border fenced (3,323 of 4,096 km)
O - OPERATIONS	**Challenge**	**Examples/Data**
Fencing	Smart fence, Tech integration	3,323 km fenced (81%); 773 km pending; CIBMS pilot projects
Surveillance	Drones, Night vision, Thermal imaging	450 drones deployed; Facial recognition at 78 checkpoints
R - REGIONAL TENSIONS	**Challenge**	**Examples/Data**
China LAC	Incursions, Infrastructure build-up	3,488 km LAC; 18 face-offs (2024); Galwan: 20 martyred
Pakistan LoC/IB	Infiltration, Ceasefire violations	308 violations; 47 infiltration attempts; 14 tunnels detected
D - DRUG TRAFFICKING	**Challenge**	**Examples/Data**

Golden Crescent	Afghanistan-Pakistan-India route	₹72,000 crore drugs seized (2020-24); Punjab: 2.3 lakh addicts
Golden Triangle	Myanmar-India route	12,400 kg heroin from Manipur border (2023); 4,000 kg meth single op

E - ESPIONAGE	**Challenge**	**Examples/Data**
Cross-border	ISI agents, Sleeper cells	127 espionage cases (2020-24); Honey-trapping 89 cases
Drone surveillance	Pak drones, Weapon dropping	187 drone sightings; 9 shot down; 51 pistols, 78 grenades dropped

R - ROUTES (Smuggling)	**Challenge**	**Examples/Data**
Arms	AK-47s, Pistols, Grenades	847 weapons seized (2023); 50 AK-47s, 200 grenades (March 2024, Uri)
FICN	Fake currency notes	₹42.43 crore seized (2023); Pakistan presses; ₹400+ crore circulation

S - SMUGGLING (Crime-Terror Nexus)	**Challenge**	**Examples/Data**
Funding	Drug money for terror operations	67% of LeT, JeM funding from drug trade; Pulwama: ₹35 lakh from drugs
Networks	D-Company, ISI, LeT collaboration	Dawood-ISI-LeT triangle; ₹500 crore annually; 1993 Mumbai blasts funded

CIBMS EVALUATION

POSITIVES	**Examples/Data**
Integrated Surveillance	Thermal imaging, underground sensors, facial recognition at 78 checkpoints
Budget	₹9,763 crore sanctioned (2018-2028); 10 pilots: Ploura (Jammu), Dharchula (Uttarakhand)
Technology	450 drones; Laser walls (pilot); Day/night cameras every 300m; Command centers
LIMITATIONS	**Issues**
Incomplete	Only 40% operational; 10 pilots sanctioned, 4 completed; 773 km Bangladesh unfenced
Technology Jamming	Pakistan jams signals; 9 drones shot down; Fog affects lasers; False alarms
Manpower Shortage	Trained operators lacking; 24x7 monitoring needs 3-shift rotation—insufficient BSF
Maintenance	Harsh weather damages; Ladakh cold, Rajasthan heat; Spare parts delays

TEMPLATE	HEADING	SUB-HEADING	SPECIFIC ACTIONS
SECURITY	**S - Strengthening**	Legal, Institutional	Bilateral treaties for cattle smuggling prosecution; Joint investigation teams for trafficking; Extradition for narcotics
SECURITY	**E - Empowerment**	Community, Village Defense	Village Defense Committees in 500 border villages; Community policing; Local informer networks with protection
SECURITY	**C - Coordination**	Real-time Intel Sharing	Unified wireless communication for BSF, Army, State Police; Joint Control Rooms at sector level; Real-time data sharing
SECURITY	**U - Upgradation**	Equipment, Communication	Anti-drone systems (counter 187 sightings); Quantum encryption to prevent jamming; Night-vision for all BOPs
SECURITY	**R - Resources**	Budget, Infrastructure	₹15,000 crore for CIBMS completion; Operationalize 4,072 mobile towers; Medical facilities at remote BOPs
SECURITY	**I - Intelligence**	Surveillance, Analysis	AI-powered threat prediction; Facial recognition expansion from 78 to 200 checkpoints; Crypto tracking for terror funding
SECURITY	**T - Technology**	AI, Blockchain, Satellites	Satellite-based 24x7 monitoring; Blockchain for trade transactions; AI analytics for pattern detection
SECURITY	**Y - Youth**	Employment, Skill	10,000 youth employed in border infrastructure; Reduce smuggling incentive through legal employment; Entrepreneurship support

---

CONCLUSION

Comprehensive border security requires technology, infrastructure, coordination, development, and diplomatic engagement.

QUESTION 5

"Despite institutional frameworks, India's internal security architecture suffers from coordination gaps and capacity deficits. Examine the challenges faced by security forces

and agencies, and suggest reforms for effective security governance." (250 words, 15 marks)

ANSWER 5

INTRODUCTION

India's security apparatus—10.5 lakh CAPF, 26.9 lakh state police, ₹1.15 lakh crore budget—faces systemic failures. 26/11 Mumbai exemplified coordination chaos when NSG, Police, Navy operated without unified command for 60 hours (166 deaths). With 78,000 vacancies, 68% outdated weapons, 50,000 BPJ shortage, and only 8 states implementing Prakash Singh reforms, capacity deficits undermine effectiveness.

BODY: CHALLENGES

Using Template 5: UNIFORMS (Unity-National-Intelligence-Forces-Operations-Reform-Modernization-Synergy)

U - UNITY OF COMMAND	Challenge	Examples/Data
Single Commander	Lack of coordination, Turf wars	26/11: NSG arrived 10 hours late; Different wireless systems; No unified command
Joint Operations	Multiple agencies, No integration	166 deaths in 60 hours; NCTC proposed 2013, shelved due to state opposition

N - NATIONAL INVESTIGATION AGENCY	Challenge	Examples/Data
Terror Cases	NIA Act 2008; Pan-India jurisdiction	1,876 cases registered; 312 ongoing (2024); Only 650 officers vs need 3,000
Conviction	Success rate vs capacity	94.7% conviction rate (state 32%); Quality high but quantity insufficient

I - INTELLIGENCE AGENCIES	Challenge	Examples/Data
Internal	IB, State intelligence, Coordination	26 state bureaus don't always share; 26/11: Intel ignored; Pulwama: Gap
External	RAW, NTRO, DIA, HUMINT deficit	Limited HUMINT in Pakistan, China; 8 attaches abroad inadequate

F - FORCES (CAPF & State Police)	Challenge	Examples/Data
Paramilitary	CRPF, BSF, CISF, ITBP, SSB, NSG, AR	10.5 lakh personnel; ₹1.15 lakh crore budget; 78,000 vacancies (7.4%)

State Police	Manpower, Equipment shortage	26.9 lakh personnel; 5.5 lakh vacancies (24%); 144 per lakh vs UN standard 222

O - OPERATIONAL CHALLENGES	**Challenge**	**Examples/Data**
Equipment	Outdated weapons, BPJ shortage	50,000 BPJ shortage; 68% weapons beyond service life; 30% vehicles not mine-protected
Training	Counter-terror, CBRN, Human rights	Only 15% CAPF CBRN-trained (need 50%); 300 CAPF suicides annually; No PTSD care

R - REFORMS	**Challenge**	**Examples/Data**
Police Reforms	Prakash Singh judgment 2006	Only 8 states compliant (18 years later); 18 partial; 4 non-compliant (WB, Telangana, Goa, Mizoram)
Accountability	HR violations, Fake encounters	1,800+ custodial deaths (2020-24); 78 fake encounter cases; Only 12 police convicted

M - MODERNIZATION	**Challenge**	**Examples/Data**
Technology	Drones, AI, Cyber capabilities	450 drones procured; NATGRID 40% operational (launched 2011—13 years)
Infrastructure	Smart borders, CIBMS, Surveillance	₹9,763 crore CIBMS but 40% done; 78 facial recognition checkpoints vs need 500

S - SYNERGY	**Challenge**	**Examples/Data**
Inter-Agency	NATGRID, NCTC (shelved), MHA coord	17 agencies under NATGRID; 11 of 17 connected; Data sharing limited
Center-State	Concurrent subject, Political issues	Police in State List; States resist central forces; J&K post-370: Better coordination

WAY FORWARD

TEMPLATE	**HEADING**	**SUB-HEADING**	**SPECIFIC ACTIONS**
SECURITY	**S - Strengthening**	NIA, Legal	Add 2,500 NIA officers; NIA branches in all 28 states; Financial investigation powers; Fast-track 312 pending cases
SECURITY	**E - Empowerment**	Community Policing	Village defense committees; Civil society partnerships; Community beat officers; Mohalla committees
SECURITY	**C - Coordination**	NATGRID, MAC, SOPs	Complete NATGRID by Dec 2025 (40% done); Expand SMACs to 300

			cities; Unified SOPs for terror response
SECURITY	**U - Upgradation**	Equipment, Weapons	₹15,000 crore for 50,000 BPJ, modern weapons; Replace 68% outdated arsenal; Mine-protected vehicles for Naxal areas
SECURITY	**R - Resources**	Manpower, Budget	Fill 78,000 CAPF + 5.5 lakh police vacancies by 2027; Increase ratio to 200 per lakh; ₹5,000 crore annual modernization
SECURITY	**I - Intelligence**	HUMINT, Technology	Revive informer networks with protection; AI predictive policing in 50 cities; Joint interrogation centers (JICs)
SECURITY	**T - Technology**	NATGRID, CCTNS, AI	Single interoperable wireless system; Facial recognition 500 checkpoints; 2,000 drone fleet; Quantum encryption
SECURITY	**Y - Youth (Personnel)**	Training, Specialization	Train 50,000 in counter-terror; 50,000 in CBRN; Cyber training for 10,000; Family postings in conflict zones

CONCLUSION

Comprehensive security governance requires institutional reforms, capacity building, technology, accountability, welfare integration.

DISCOVER YOUR "PATH TO SUCCESS" WITH INDIA'S PREMIER

"TOP NOTCH ACADEMY"

Learn from the best teachers & join the ranks of our excellent results


Akash Sir


Kamal Sir

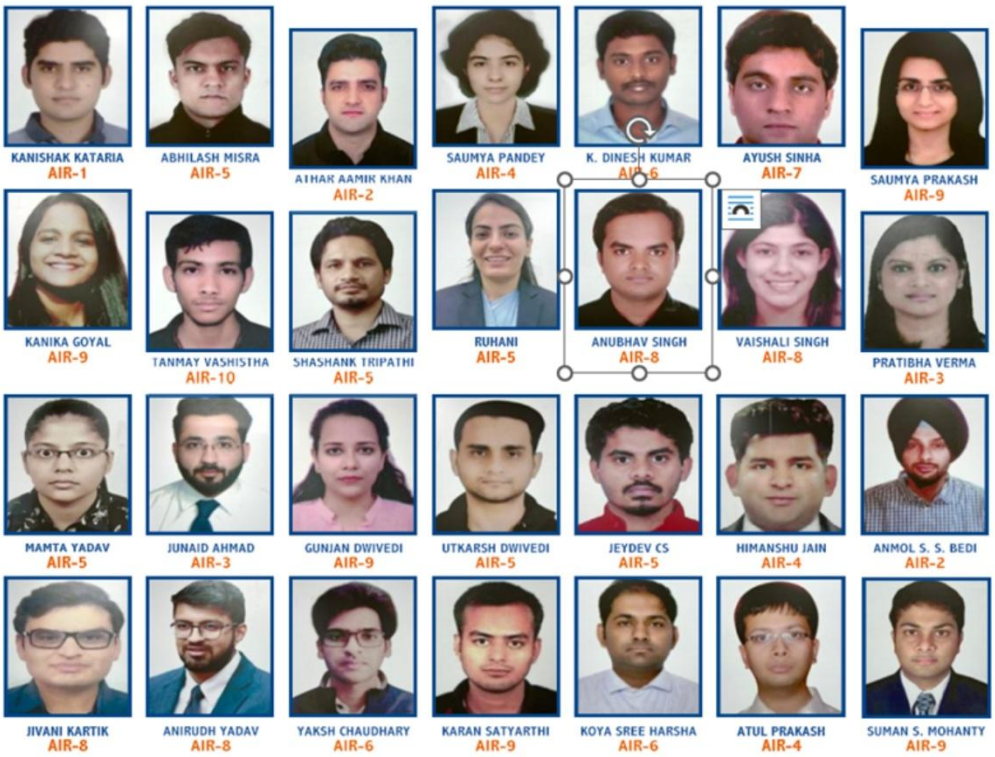

Abhishek Gaur Sir


Anand Mohan Sir


Abhishek Bhore Sir

OUR RANKERS

TOP 10 IN CIVIL SERVICES EXAMINATION



CHANAKYA
IAS ACADEMY
Nurturing Leaders of Tomorrow
SINCE 1993

CHANAKYA IAS ACADEMY

32+ Years of Excellence, More than 5500+ Selections so far

announces its batches

IAS/IFS/IPS
HCS/HAS/PCS

UPGRADED FOUNDATION COURSE

A Complete solution for prelims Mains & Interview

Scan QR Code for Registration

AVAIL FREE DEMO CLASS

CHANDIGARH CENTRE
Plot No. 8, Ground Floor, Sector 25-D,
Punjab Kesari Building, Chandigarh

8264199959

www.chanakyaiasacademychd.com