INTERNAL SECURITY –

General Concepts

1. Internal security architecture
2. National security doctrine
3. Proxy war
4. Asymmetric warfare
5. Hybrid warfare
6. Intelligence-led policing
7. Counter-insurgency (COIN)
8. Counter-terrorism (CT)
9. Security–development nexus
10. Whole-of-government approach

Terrorism & Insurgency

11. Cross-border terrorism
12. Narco-terrorism
13. Radicalisation
14. Online jihad / cyber radicalisation
15. Terror financing networks
16. FATF compliance
17. Grey zone warfare
18. Foreign terrorist fighters (FTF)
19. Over-ground workers (OGW)
20. Left-Wing Extremism (LWE)

Border & Coastal Security

21. Smart fencing (CIBMS)
22. Border Management Post (BMP)
23. Riverine border security
24. Hot pursuit (cross-border doctrine)
25. Coastal radar surveillance chain
26. EEZ (Exclusive Economic Zone)
27. SAGAR (Security and Growth for All in the Region)
28. Coastal community policing
29. Maritime domain awareness (MDA)
30. Joint Coastal Security Exercise "Sagar Kavach"

Organised Crime & Money Laundering

31. Trade-based money laundering (TBML)
32. Hawala networks
33. Black economy–crime nexus
34. Financial Intelligence Unit (FIU-IND)
35. Unlawful Activities (Prevention) Act (UAPA)
36. Prevention of Money Laundering Act (PMLA)
37. Narco routes (Golden Crescent, Golden Triangle)
38. Arms trafficking
39. Dark web marketplaces
40. Crypto-based laundering

Cyber Security

41. Critical information infrastructure (CII)
42. CERT-In (Computer Emergency Response Team – India)
43. Cyber hygiene
44. Phishing, ransomware, zero-day attack
45. Deepfakes in misinformatio
46. National Cyber Security Strategy (draft)
47. Cyber Surakshit Bharat
48. Data localisation
49. Indo-US Cyber Cooperation
50. Cyber deterrence doctrine

ONE PAGER overview

Keywords / Core Concepts

Terrorism & insurgency, cyber threat & cybercrime, cross-border militancy, "proxy warfare", law enforcement & intelligence, radicalization, border security, technology in surveillance.

Important Facts & Data Points

1. In FY 2024, India lost ₹22,845.73 crore to cyber frauds—a 206% jump from 2023 losses of ~₹7,465.18 crore.
2. CloudSEK report (2024): India was the second most-targeted country globally in terms of cyber attacks—95 Indian entities under data theft incidents; over 850 million citizen data records leaked from Hi-Tek Group, Star Health, Allied Insurance.
3. India detected 369 million malware events between October 2023 and September 2024; that is ~702 potential threats per minute on average.
4. Comparatively, US: in first half of 2022, ~53.35 million US citizens affected by cyber crime. Also US organisations suffer ~46% of global cyberattacks in certain periods.
5. Terrorism: Recent example — the Pahalgam attack in 2025 where 26 civilians (tourists + locals) were killed by Lashkar-e-Taiba / TRF militants.

Analytical Points

- Nature & Trends: Internal security threats today are multi-dimensional. Apart from traditional terror/insurgency (Kashmir, Northeast, Maoist belts), cyber threats (frauds, data theft, malware) are scaling rapidly. Low physical casualties but huge economic loss and erosion of trust.
- omparative Insight: While the US has more robust cyber infrastructure, it also has higher exposure. India's losses are rapidly catching up because of rising digital adoption but relatively weak cyber law implementation and awareness. Many attacks go unreported or lack transparency.
- Key Drivers
  - Proliferation of digital payments & low barriers → more fraud attempts.
  - Socio-economic grievances, underdevelopment → fertile ground for insurgency and radical movements.
  - Cross-border sanctuaries, proxy support in case of militancy.
  - Use of technology by both state and non-state actors (drones, social media, AI, encrypted communication).
- Weaknesses / Vulnerabilities
  - Fragmented jurisdiction among agencies.
  - Gaps in cyber literacy, law enforcement capacity, forensic infrastructure.
  - Delays in legal reform (Data Protection, stronger cyber laws).
  - Border security in rugged terrain, infiltration, radicalization.

Examples / Case Studies

- Pahalgam Attack (2025, J&K) – killings of tourists, showing continued threat of cross-border proxy militancy.
- CloudSEK & Malware Events – illustrating scale and speed of cyber attacks in India.

Conclusion / Closing Line

Internal security today is not just about borders or insurgents; it's equally about the invisible fronts—cyber, fraud, radicalization. For India to secure its citizens, it must combine technological readiness, legal strength, and grassroots intelligence with swift law enforcement.

1. Terrorism & Insurgency

Keywords: Cross-border terrorism, radicalisation, proxy war, Left-Wing Extremism (LWE), Northeast insurgency.

Data Points

1. Global Terrorism Index 2023 – India ranked 13th, behind Afghanistan (1st) and Pakistan (6th).
2. Terrorism incidents in India have declined by 77% since 2010, but sporadic high-impact attacks persist (Ministry of Home Affairs).
3. US spends ~$80 billion annually on counter-terrorism and homeland security, vs India's ₹1.6 lakh crore ($20B) internal security budget.
4. LWE violence fell from 2,258 incidents in 2009 to 600 in 2022.
5. China faces separatism in Xinjiang but uses mass surveillance; India focuses on democratic engagement + development.

Examples: Pahalgam attack (2025); decline of LWE under SAMADHAN strategy; surrender of insurgents in Northeast after peace accords.

Conclusion: Terrorism in India is sustained by external sanctuaries and internal grievances—resolving it needs a blend of force, dialogue, and development.

2. Left-Wing Extremism (LWE)

Keywords: Red Corridor, SAMADHAN

strategy, Greyhounds, security–

development nexus. Data Points

1. LWE incidents down by over 75% between 2010–2022 (MHA).
2. Only 45 districts are now severely affected, down from 96 in 2010.
3. India spends ~₹3,000 crore annually on LWE security ops; China spends far higher on Xinjiang security.
4. BRICS: Brazil also battles organised crime–violence nexus, similar structural roots.
5. Over 5,000 Maoist cadres surrendered since 2014.

Examples: Greyhounds' success in Andhra; Bastar operations in Chhattisgarh.

Conclusion: LWE is shrinking geographically, but social justice, tribal rights, and inclusive growth are the only sustainable antidotes.

3. Border Management

Keywords: Riverine borders, fencing, infiltration, smuggling, drone threats.

Data Points

1. India has 15,106 km of land border + 7,516 km coastline.
2. 3,323 km with Pakistan, 3,488 km with China; porous borders with Nepal, Myanmar.
3. Riverine borders in Assam–Bangladesh remain unmanned; contrast with US-Mexico where 580 miles of fencing exists.
4. China invests heavily in border infrastructure (e.g., Tibet highways), while India's Vibrant Villages Programme is still scaling up.
5. Smuggling: seizure of contraband worth ₹3,000+ crore in 2023 along NE borders.

Examples: BSF drone interception in Punjab; fencing along Bangladesh border reducing illegal migration.

Conclusion: Borders are the first line of internal security—India must integrate technology with community cooperation.

4. Organised Crime & Terror Linkages

Keywords: Money laundering, narco-terrorism, hawala, arms trafficking.

Data Points

1. UNODC estimates 2–5% of global GDP ($800B–$2T) is laundered annually.
2. India reported ₹10,500 crore+ suspicious transactions in 2022 (FIU).
3. Trade-Based Money Laundering (TBML) in India often linked with gold smuggling.
4. Pakistan's terror financing grey-listing by FATF (2018–2022) reduced its terror groups' funding.
5. US DEA regularly reports narco-funding of cartels; India faces similar challenges in Punjab & Northeast.

Examples: Mumbai underworld's historic terror links; heroin smuggling via Golden Crescent.

Conclusion: Organised crime is no longer local; transnational cartels fund terror—India must strengthen FIU, FATF compliance, and regional cooperation.

5. Cyber Security

Keywords: CERT-In,

ransomware, phishing, AI-

driven threats, data

localisation. Data Points

1. India reported 13.9 lakh cyber incidents in 2022 (CERT-In).
2. India is 2nd most targeted nation globally after USA (CloudSEK 2024).
3. Average cost of data breach in India: ₹17.9 crore (IBM report, 2023).
4. US has ~1 million+ cyber workforce; India ~3 lakh, reflecting capacity gap.
5. China runs the world's largest cyber army—over 50,000 hackers linked to PLA units.

Examples: Mumbai power outage (2020) linked to suspected cyber intrusion; ransomware attacks on AIIMS in 2022.

Conclusion: Cyber is the new battlefield—India must blend legal reforms, workforce skilling, and global cooperation to stay secure.

6. Terror Financing & Money Laundering

Keywords: Hawala, TBML (Trade-Based Money Laundering), narco-terrorism, FATF compliance.

Data Points

1. UNODC: Terror groups generate $1.6 trillion annually globally from organised crime (≈2–5% of world GDP).
2. India reported ₹10,500+ crore suspicious transactions in 2022 (FIU).
3. Pakistan was on FATF grey list (2018–2022) → terror funding inflows fell ~30% during that period.
4. USA PATRIOT Act gives sweeping powers to choke illicit financing—India's PMLA is narrower.
5. China faces terror-finance watchlists in Xinjiang but uses strict banking surveillance.

Examples: D-Company hawala networks in Mumbai; heroin smuggling through Punjab.

Conclusion: Stronger FIU, global cooperation, and strict FATF compliance are essential to cut the financial lifelines of terror.

7. Radicalisation & Fake News

Keywords: Online radicalisation, social media echo chambers, deepfakes, psychological warfare.

Data Points

1. 77% of Indians receive news via WhatsApp (Reuters Institute, 2023).
2. US Capitol riots (2021) show impact of fake news on democracy; India saw 2020 Delhi riots fuelled by misinformation.
3. India reported ~7,400 fake news cases in 2022 (MHA).
4. China runs a "Great Firewall", while India balances freedom of speech vs regulation.
5. BRICS: Brazil also battles WhatsApp-based misinformation during elections.

Examples: Deepfake videos during recent state elections; communal flare-ups from fake WhatsApp forwards.

Conclusion: Radicalisation today spreads faster through bytes than bullets—digital literacy + swift fact-checking is the real antidote.

8. Drone Warfare & Smuggling

Keywords: UAV,

swarm drones,

payload delivery, AI-

enabled surveillance.

Data Points

1. BSF detected 280+ drone intrusions along the Pakistan border in 2022.
2. Each drone can carry up to 10 kg of arms, drugs, or IEDs.
3. China is the world's largest drone manufacturer (DJI holds 70% of global market).
4. US military pioneered drone warfare post-2001; India is catching up with projects like SWARM drones (IAF 2021).
5. Cross-border drones dropped 80 kg of heroin in Punjab (2023).

Examples: Jammu Air Force Station drone attack (2021).

Conclusion: India must combine counter-drone tech, electronic warfare, and community policing to secure its skies.

9. Coastal & Maritime Security

Keywords: Blue economy,

EEZ, piracy, smuggling,

UNCLOS.

Data Points

1. India has 7,516 km coastline, 1,382 islands, 2.3 million sq km EEZ.
2. Mumbai 26/11 exposed gaps in coastal security; led to CISF/Marine Police strengthening.
3. India's blue economy potential = $1 trillion by 2035 (NITI Aayog).
4. US Navy operates 11 carrier strike groups worldwide; India has 2 functional aircraft carriers.
5. China's PLAN has the world's largest navy (370+ ships) and presence in IOR via Djibouti base.

Examples: Coastal radar chain; SAGAR (Security & Growth for All in the Region).

Conclusion: India's coastal frontiers are both economic highways and security frontlines—robust surveillance, fishermen integration, and Indo-Pacific partnerships are the key.

10. Institutional Framework & Reforms

Keywords: NIA, UAPA, NCTC, NATGRID, coordination.

Data Points

1. NIA convicted rate: over 90%, one of the highest globally.
2. US created DHS after 9/11; India still lacks a centralised counter-terrorism agency like NCTC.
3. India's police-population ratio: 156 per lakh vs UN norm of 222; USA ~238, China ~170.
4. Cybercrime police stations in India: <400 nationwide (vs 18,000+ in US FBI field offices).
5. NATGRID connects 11 databases across 21 agencies, but implementation delays persist.

Examples: NIA crackdown on ISIS cells; NATGRID used in drug trafficking probes.

Conclusion: India needs modernisation of police, tech-driven intelligence, and seamless inter-agency coordination for effective internal security.