VISIONIAS
INSPIRING INNOVATION

SECURITY

Classroom Study Material 2025

June 2024 to June 2025

MAINS 365

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

8468022022
9019066066

enquiry@visionias.in /c/VisionIASdelhi /visionias_upsc vision_ias /VisionIAS_UPSC www.visionias.in

SECURITY

Table of Contents

1. STATE AND NON-STATE ACTORS _____ 7

1.1. Left Wing Extremism at a Glance _____ 7

1.1.1. Urban Naxalism _____ 8

1.2. Insurgency in Northeast at a Glance ___ 9

1.3. Armed Forces Special Powers Act (AFSPA), 1958 _____ 9

1.4. Keywords _____ 10

1.5. Practice Question _____ 11

2. THREATS TO INTERNAL SECURITY _____ 12

2.1. Technology and Internal Security _____ 12

2.1.1. Online Radicalisation at a Glance _____ 12

2.1.2. Social Media Influencers' and National Security _____ 13

2.1.3. Crypto Currency Hawala Nexus _____ 13

2.1.4. Role of Quantum Computing in National Security _____ 15

2.2. Data Protection at a Glance _____ 16

2.2.1. Digital Personal Data Protection Act (DPDP), 2023 _____ 17

2.2.2. Facial Recognition Technology _____ 18

2.3. Cyber Security At A Glance _____ 19

2.3.1. United Nations Convention on Cybercrime19

2.3.2. Critical Information Infrastructure at a Glance _____ 21

2.4. Geospatial Data and National Security at a Glance _____ 22

2.5. Money Laundering and Smuggling ____ 23

2.5.1. Money Laundering and Terrorist Financing (ML/TF) _____ 23

2.5.2. Financial Action Task Force (FATF) _____ 24

2.5.3. Drug Trafficking in India At A Glance ___ 26

2.6. Terrorism _____ 27

2.6.1. Terrorism In India at a Glance _____ 27

2.6.2. India's New Security Doctrine_____ 27

2.6.3. India's Diplomatic Outreach Against State Sponsored Terrorism _____28

2.6.4. Transnational Organised Crimes at a Glance _____30

2.7. Emerging Dimensions of Warfare _____31

2.7.1. Adaptive Defense and Frontier Technologies in Modern Warfare _____31

2.7.2. Hybrid Warfare at a Glance _____33

2.8. Space Weaponization at a Glance _____34

2.9. Keywords _____35

2.10. Practice Question _____35

3. SECURITY CHALLENGES AND THEIR MANAGEMENT IN BORDER AREAS _____36

3.1. Security Issues in Border Areas _____36

3.1.1. Border Security at a Glance _____36

3.1.2. 25 years of Kargil War _____37

3.2. Maritime Security _____39

3.2.1. Maritime Security at a Glance _____39

3.3. Keywords _____40

3.4. Practice Question _____40

4. SECURITY FORCES _____41

4.1. Defence Modernisation _____41

4.1.1. Modernisation of Armed Forces at a Glance _____41

4.1.2. Defence Exports at a Glance _____42

4.1.3. Integrated Theatre Commands (ITCs) ___42

4.1.4. Indian Coast Guard _____43

4.1.5. National Investigation Agency (NIA) ____44

4.1.6. Forensics In India _____45

4.2. Global Agencies _____46

4.2.1. INTERPOL _____46

4.3. Keywords _____47

4.4. Practice Question _____48

5. MISCELLANEOUS _____49

5.1. Rise in Nuclear Weapons Arsenal _____ 49

5.2. 25 years of India's Nuclear doctrine ___ 50

5.3. Biological Weapons Convention (BWC) 51

5.4. Drones for Defense at a Glance _____ 53

5.5. Fifth-Generation Fighter Jet AMCA ___ 54

5.6. India's Air Defence System (ADS) _____ 55

5.7. Multiple Independently Targetable Re-entry Vehicle (MIRV) Technology _____ 56

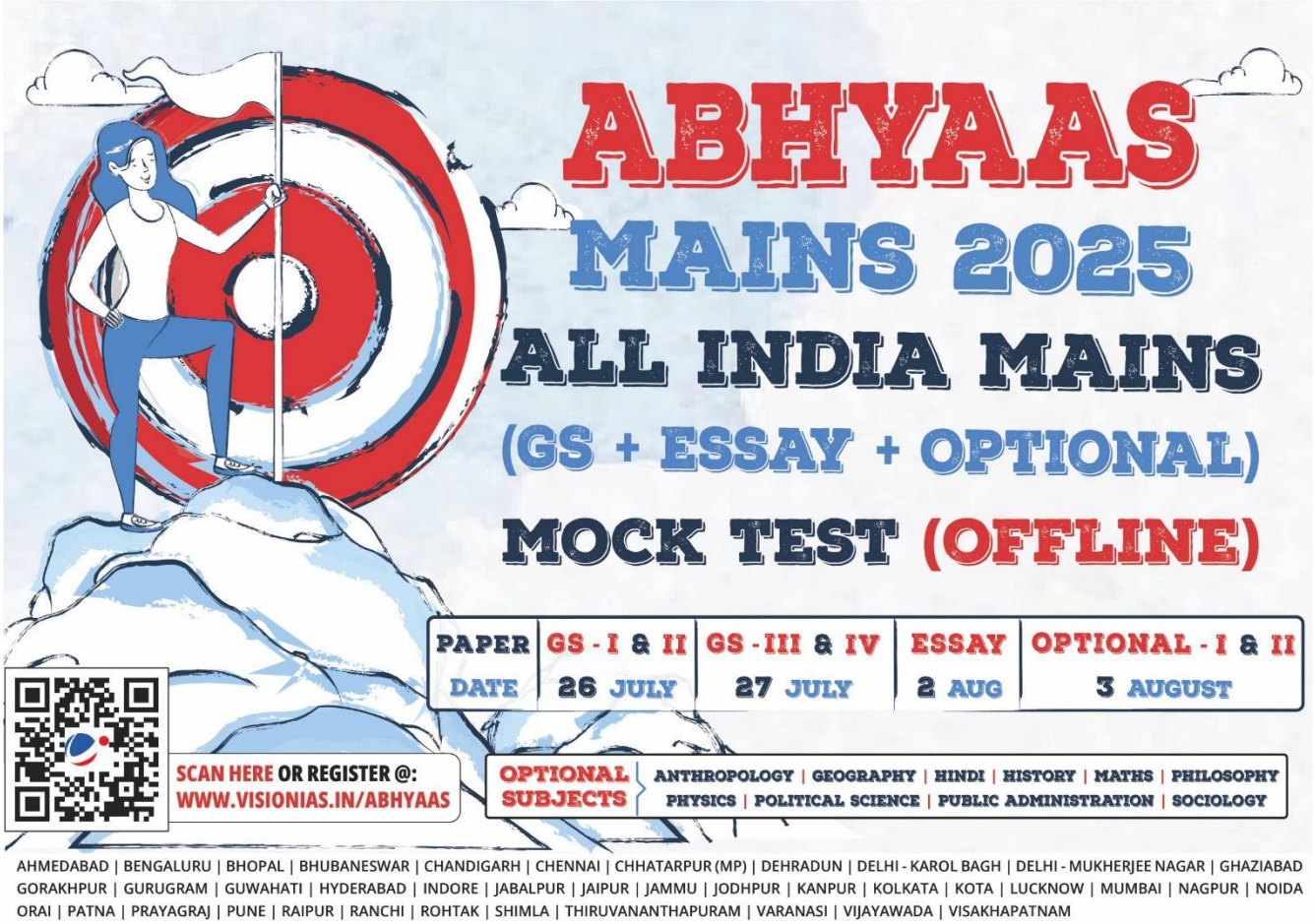
5.8. Directed Energy Weapons _____56

5.9. Keywords _____57

5.10. Practice Question _____58

6. SECURITY PREVIOUS YEAR QUESTIONS 2013-2024 (SYLLABUS-WISE)_____59

7. APPENDIX: KEY DATA AND FACTS62



AHMEDABAD | BENGALURU | BHOPAL | BHUBANESWAR | CHANDIGARH | CHENNAI | CHHATARPUR (MP) | DEHRADUN | DELHI - KAROL BAGH | DELHI - MUKHERJEE NAGAR | GHAZIABAD
GORAKHPUR | GURUGRAM | GUWAHATI | HYDERABAD | INDORE | JABALPUR | JAIPUR | JAMMU | JODHPUR | KANPUR | KOLKATA | KOTA | LUCKNOW | MUMBAI | NAGPUR | NOIDA
ORAI | PATNA | PRAYAGRAJ | PUNE | RAIPUR | RANCHI | ROHTAK | SHIMLA | THIRUVANANTHAPURAM | VARANASI | VIJAYAWADA | VISAKHAPATNAM

Copyright © by Vision IAS

All rights are reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of Vision IAS.

Preface

To the Aspirant Who Dares to Dream

In the quiet corners of libraries across India, in the solitude of late-night study sessions, and in the hearts of millions who dare to dream of serving the nation, lies an unwavering determination to crack one of the world's most challenging examinations – the UPSC Civil Services Examination.

Mains 365 was born from that very spirit of determination and the recognition that success in UPSC CSE Mains 2025 demands more than just hard work; it requires strategic preparation, comprehensive understanding, and the ability to connect diverse streams of knowledge into coherent, impactful answers.

Q.1 Why most of UPSC aspirants fail to crack mains?

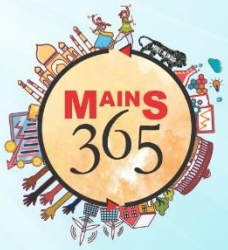
- **Scattered Information:** Jumping between multiple sources creates confusion
- **Outdated Content:** Using materials that don't reflect current developments
- **Lack of Integration:** Inability to connect static knowledge with current affairs
- **Poor Answer Structure:** Not knowing how to present knowledge effectively
- **Missing the UPSC Mindset:** Failing to understand what UPSC actually want

But what if you could overcome ALL these challenges with ONE comprehensive resource?

Q2. Why Mains 365 Security?

It is a one-stop annual compendium that distils every high-stakes current-affairs themes like new counter terrorism doctrine —into exam-ready notes mapped topic-by-topic to the UPSC CSE Mains syllabus.

Also, Security Mains 365 document enriches multiple GS papers—e.g., GS-2 (welfare schemes in bordering areas (VIBRANT VILLAGE PROGRAMME), GS-III (recent advancement in defense technologies), and GS-IV (ethical issues with violation of Fundamental rights in disturbed areas).



Q3. How does it mirror the General Studies papers?

Chapters are mapped after syllabus topics and recurring themes in the UPSC exam like State and non-state actors, Threats to internal security includes terrorism and emerging dimension of warfare and security challenges and their management in bordering areas.

Q4. I already have static books. Why do I need this?

Static concepts fetch marks only when linked to real examples. Mains 365 does this by connecting the year's key trends, data, committee (Bandopadhyay, Justice Verma, etc.), reports like the World Drug Report, examples, etc.—making your answers sharper, richer, and more analytical. We have also added a keyword at the end of every chapter, which will make the recollection of security-specific words easier

Q5. Will it actually save me time in the exam hall?

Yes. Infographics, definitions, and "Why in News" sections act like visual flashcards, you recall a picture, not a paragraph, that saves minutes off every 10- or 15-marker.

2.7.1. ADAPTIVE DEFENSE AND FRONTIER TECHNOLOGIES IN MODERN WARFARE

Why in the News? → **CAN BE USED AS INTRODUCTION**

The Defence Minister stressed the need for an **'Adaptive Defense' strategy** to deal with fast-changing threats from **emerging and frontier technologies.**

What Are Frontier Technologies?

- They are fast-evolving innovations driven by **digitalization and connectivity.**
- **They could be:**
  Digital: AI, IoT, Metaverse, Quantum
  Physical: 3D printing
  Biological: Bioprinting, genetic engineering

What is Adaptive Defense?

- **Definition:** A **strategic approach** where **defence systems evolve continuously** to counter emerging threats.
- **Core Principle:** Emphasizes a **proactive mindset** to anticipate, adapt, innovate, and respond effectively to unpredictable security challenges.

DEFINITION

CAN BE USED AS VALUE ADDITION

Steps taken by India for adopting Frontier Technologies

- **Establishment of Defence AI Council (DAIC)** and Defence AI Project Agency (DAIPA)
- **Project Seeker:** AI-based facial recognition, surveillance, monitoring system of Indian Army
- **'Antariksha Abhyas – 2024':** First Ever Space Exercise to integrate India's space capability in military operations.
- **DRDO Young Scientists' Laboratories:** To provide solutions in advanced technology areas of warfare.

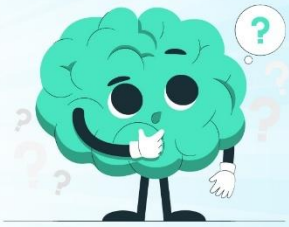
Q6. What gives my answers extra credibility?

Ready-to-use definitions, latest data from **recent reports** (e.g., World Drug Report 2024) and recommendations from **official sources** (e.g., Ministry of Home Affairs), **key committees'** recommendations like Madhukar Gupta, Shekatkar Committee, **key facts** (e.g., 81% reduction in incidents of LWE violence between 2010 and 2024) embed instant authority. UPSC love precise references.

Q7. How is it structured for the 3-hour examination?

Every sub-topic follows the golden sequence—Context → Analysis → Way Forward—so you can lift the framework, plug in your insights, and write at full speed while others are still outlining.

Q8. Can you demonstrate with an actual question?



PYQ: "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 10 Marks))"

Quick extract from Mains 365 → LWE at a glance

- Definition of Left-Wing Extremism and current trend.
- Approach of the government to address challenged posed by LWE
- Conclusion: Acknowledge the positive impact of the multi-pronged approach by highlighting the need for sustained efforts and community engagement.

Plug these into Intro–Body–Conclusion:

Start by defining LWE, quote data for the declining trend, highlight government approaches like security related, developmental related etc.

Result will be a focused, 150-word answer that links recent data and standard guidelines to theory—just what UPSC looks for in a 10-mark question.

Q9. What's the recommended micro-structure for each 15 marker?

- Intro (≤30sec): Why in the News, or data/facts.
- Body (≤6min): 2–3 dimensions, each with evidence & analysis.
- Way forward (≤1min): 3–4 actionable reforms.
- Conclusion (1 line): Memorable, visionary sentence.

Q10. Any final pro tip?

Think of Mains 365 as a ready-made answer bank: it's pre-curated—your job is to pick, organize, and add your own insight. Use it wisely, and you'll find questions easier to answer and higher marks more achievable.

Best Wishes,

Team VisionIAS

1. STATE AND NON-STATE ACTORS

1.1. LEFT WING EXTREMISM AT A GLANCE

Left Wing Extremism (LWE)

- LWE known as **Naxalites in India and Maoists globally**.
- **Follows Maoist ideology**, promotes violence to overthrow democratic government.
- Began with the **1967 Naxalbari uprising** in West Bengal. India aims to **eliminate it by March 2026**.

Red Corridor	Current Spread of LWE	Achievement in containing
The region affected by LWEs **is referred to as Red Corridor in India.**	Only **6 districts are most affected by Naxalism** and only **18 districts are Naxal-affected** in 2025 against 35 and 126 in 2014 (respectively)	81% reduction in incidents of LWE violence between 2010 and 2024.

Factors responsible for emergence Of LWE

Jal, Jungle, Jameen (Water, Forest and Land)	Socio-Economic Inequalities	Inadequate implementation of government policies
Expropriation of resources by outsiders, evasion of land ceiling laws	Inequalities in basic services like health, education, roads, and as lack of employment opportunities	Jharkhand is yet to implement Provisions of the Panchayats (Extension to the Scheduled Areas) Act or PESA, 1996

Reasons for decline in LWE Spread in India

Strengthened Security Architecture

- **National Policy and Action Plan (2015):** Based on the zero-tolerance approach towards Naxalism.
- **SAMADHAN Strategy:** Provides 8 Pillars to tackle LWE (**S**mart Leadership, **A**ggressive strategy, **M**otivation and training, **A**ctionable intelligence, **D**ashboard based KPIs, **H**arness technology, Action plan for each theatre, **N**o access to financing)
- **'Modernization of Police Forces'** Operation Octopus, Operation Double Bull, etc.

Developmental

- **178 Eklavya Model Residential Schools** functional in LWE-affected districts.
- **Special Central Assistance (SCA),** Financial Inclusion,Skill & Education,Dharti Aaba Abhiyan

Community Engagement

- Civic Action Programme (CAP) to bridge the gaps between Security Forces and local people

Challenges persist in containing LWE

Trust Deficit	Misuse of technology	Difficult Terrain	Security Infrastructure
Cultural differences and perceptions reduce local trust in security and administration	Non-state actors **use Dark web** to create fake news to malign government, recruit members, **virtual currencies** for money laundering, etc.	Continuous forest terrain of states like Jharkhand, Chhattisgarh, Orissa	limited intelligence coordination, Easy access to weapons through illegal arms manufacturers, etc.

Way ahead to tackle LWE

Bridging Trust Deficit	Countering ideology	Security and Capacity building	Other
Ensure tribal-friendly land acquisition and rehabilitation policies **(Bandyopadhyay Committee).** Measures like **the Forest Rights Act, 2006,** should be carefully applied	Promote **constitutional democracy** to counter violent Maoist ideology	Focus on modernizing local police and using smart, **intel-led units like the Greyhounds for better results**	Centre-state coordination,Use of Technology like GIS and GPS

1.1.1. URBAN NAXALISM

Why in the News?

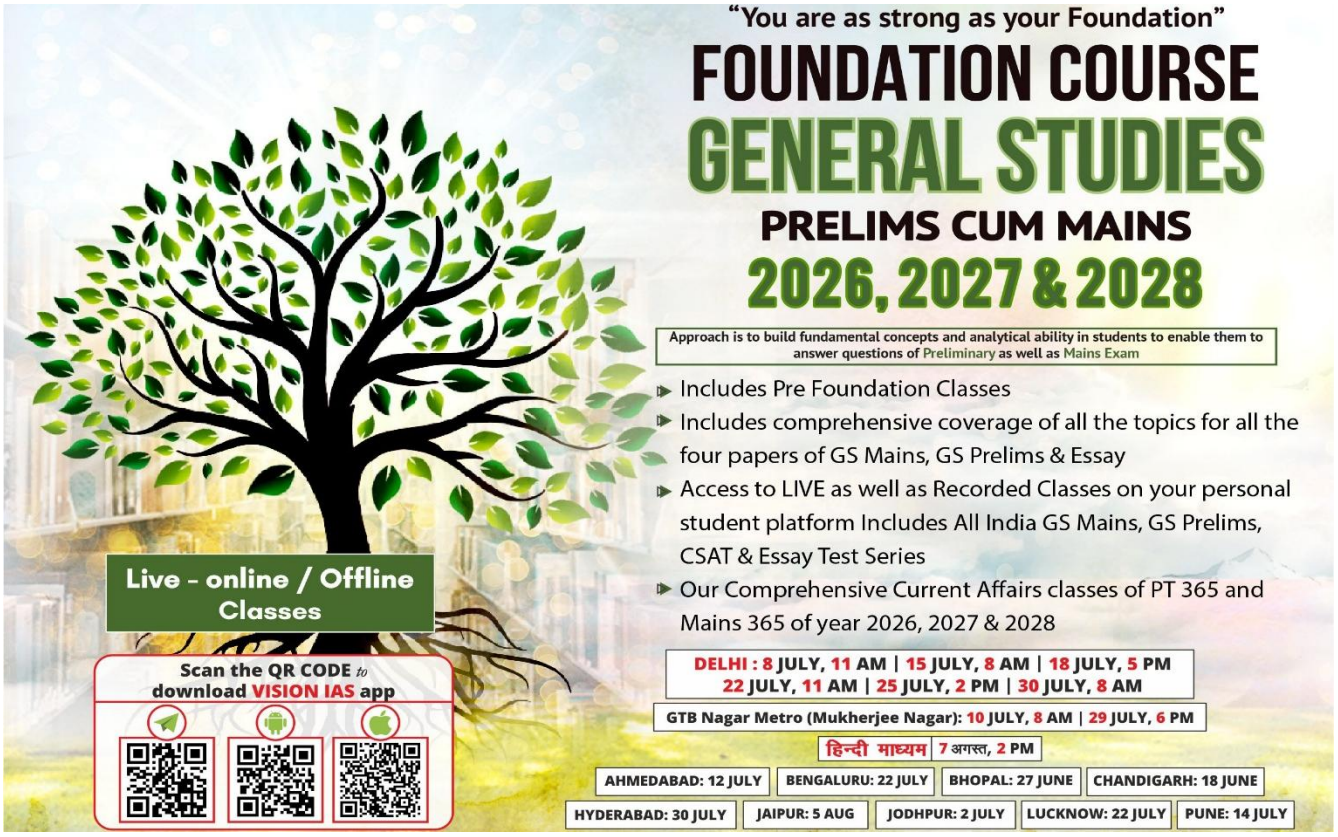
Prime Minister expressed that decisive government actions have cleared Naxalism from the jungles, but it is now spreading to urban centres.

About Urban Naxalism

- Urban Naxalism refers to **Maoists operating in cities through front organizations** that appear legitimate but actually support the CPI (Maoist) party.
- Guided by the **Strategies and Tactics of Indian Revolution (STIR) document,** these groups **operate covertly to spread Maoist ideology,** particularly among youth, students, women, and minorities **by promoting a sense of victimhood.**
- These front groups **hide the violent nature of Maoist ideology** by:
  - Operating under the **cover of democratic movements**
  - **Spreading propaganda a**nd misinformation
  - **Building alliances** with other insurgent groups
  - Sometimes **receiving support from foreign forces opposed to India**
- Their **key functions** include
  - **Recruitment** of 'professional revolutionaries',
  - **Raising funds** for the insurgency,
  - Creating **urban shelters f**or underground cadres,
  - **Providing legal assistanc**e to arrested cadres and mass- mobilisation by agitating over issues of relevance/ convenience.

Conclusion

Urban Naxalism hinder the nation's progress by targeting key infrastructure and development initiatives and keeping communities in poverty. However, in modern, aspirational India, violent ideologies have no place. The real way forward lies in inclusive development and peaceful democratic engagement.



1.2. INSURGENCY IN NORTHEAST AT A GLANCE

Insurgency

Insurgency is a violent attempt to oppose a country's government which is carried out by citizens of that country

Reasons behind Insurgency in Northeast India

Large scale **ethnic rivalries** with neighboring tribes. E.g., Meitei vs Kukis in Manipur	**Sense of alienation** from mainstream due to presence of security forces under AFSPA	**Territorial Conflicts:** For example, the **Assam-Mizoram Border Dispute**	**Militant group rivalries** For example, rivalries in NSCN-Muivah and NSCN- Khaplang factions, complicates Naga talks	**Porous international borders** facilitating arms smuggling and illegal migration	**Lack of effective governance** E.g. Shortage of medical facilities, inadequate housing in Nagaland

Initiatives taken to restore Peace in Northeast

Peace deal/Settlement agreements	Strategic Connectivity	Infrastructure	Cultural Connect	Regional Cooperation
National Liberation Front of Tripura Agreement, Bodo Peace Accord, Karbi Anglong Peace Agreement.	UDAN scheme, Rail upgrades (Vande Bharat Express) **Major bridges/ tunnels** (Bogibeel, Dhola Sadiya, Metri Setu, Sela Tunnel)	India's first **National Sports University** in Manipur **AIIMS** in Assam Aspirational District programme	Inclusion of the **Moidams of Choraideo** on UNESCO's World Heritage list. **Ashtalakshmi Mahotsav:** Showcased Northeast's textiles, tourism, GI-tagged products, and crafts	Shift from **"Look East" to "Act East"** policy Agartala–Akhaura rail link with Bangladesh, and **Kaladan Transit,**

Way ahead to ensure peace in Northeast India

Political Amend North Eastern Council Act 2002 to restore conflict resolution provision'	**Socio-cultural Connect** Cultural exchanges to raise awareness about Northeast	**De-securitization Replace** border militarization with cross border cooperation	**Security** counter-insurgency should be complemented with Peace efforts and human rights protection	**Economic Opportunities** Promote agro-processing, bamboo-based industries	**AFSPA Act** Implement **Santosh Hegde Committee (2013)** and **Justice Verma Committee** (2013) recommendations.

1.3. ARMED FORCES SPECIAL POWERS ACT (AFSPA), 1958

Why in the News?

Ministry of Home Affairs reimposed **Armed Forces (Special Powers) Act (AFSPA), 1958** in **"disturbed areas"** of Manipur including Jiribam.

Key highlight of AFSPA

- **Disturbed areas:** A **part or whole** state/UT can be declared so by **Governor** of state, **administrator** of UT or by **Centre** if u**se of armed forces in aid of civil power is necessary** to restore order.
- **Grants Special power to armed forces:** They can **open fire** against any person in contravention of law, arrest and search premises without warrant, etc.

- **Immunity to Armed Forces personnel:** Prohibits legal proceedings against them **except with the previous sanction** of the Central Government.
- **Treatment of arrested person**: Army authority is required to **handover** the arrested person to the officer-in-charge of the **nearest police station** with **least possible delay.**
- **Applicability:** Parts of Assam, Manipur, Nagaland, Arunachal Pradesh.
  - **Armed Forces (Jammu & Kashmir) Special Powers Act 1990** is applicable to disturbed areas of Jammu and Kashmir.

Other Related Information about AFSPA

- **Supreme Court Judgements**
  - **Naga People's Movement for Human Rights Case (1997):** Court held power to cause death is to be exercised under definite circumstances.
  - **Extra Judicial Execution Victim Families Association case (2016):** Court ruled that **armed forces could not be immune from investigation for excesses committed** during discharge of their duties even in **disturbed areas**.
- **Committees Recommendations**
  - **Justice B.P. Jeevan Reddy Committee (2004)** recommended scrapping AFSPA.
  - **Santosh Hegde Committee (2013)** suggested review of the Act every six-month.
  - **Justice Verma Committee (2013)** called for subjecting sexual violence against women by armed forces to regular criminal law.

Concerns with AFSPA

- **Violation of Fundamental Rights:** It infringes on constitutional rights such as **Article 19,21 and 22** etc.
- **Lack of Accountability**: The law gives armed forces wide powers and protects them from being prosecuted, leading to cases of **abuses like extrajudicial killings and rape**.
- **Militarization of Governance:** The law encourages **military dominance**, weakening democratic civilian control in conflict zones.
- **Centre-State Tensions**: AFSPA undermines **state autonomy** by allowing the central government to impose restrictions even when the situation may not warrant it.
- **Contravention of International Law:** AFSPA breaches **international human rights** treaties like UDHR, ICCPR, and the Convention against Torture.

Way Forward

- **Ensure Accountability:** Security forces must follow Supreme Court and committee guidelines.
- **Promote Dialogue:** Engage with affected communities to build trust and address concerns.
- **Use AFSPA Selectively:** Apply it only in specific troubled districts, not entire states.
- **Explore Alternatives:** Focus on development, services, and solving root causes of conflict.

Conclusion

The reimposition of AFSPA in Manipur highlights security concerns but raises serious human rights and accountability issues. A balanced and accountable use of the Act is key to addressing conflict while protecting democratic values.

1.4. KEYWORDS

Keywords				
Democratic state structure	Red Corridor	Jal,Jangal and Jameen	Socio-Economic Inequalities	Trust Deficit
Constitutional Democracy	Centre-State Coordination	Capacity building	Alienation	Strategic Connectivity
Cultural Connect	De-securitisation	Disturbed Ares	Immunity	Fundamental Rights

Human Rights	Extra-judicial execution	State Autonomy	Accountability	Militarization of Governance

1.5. PRACTICE QUESTION

Answer Canvas

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.

Introduction	Body Part: 1	Body part: 2	Conclusion
Provide data showing decline in LWE and Mention current spread of LWE	Highlight persisting challenge in countering LWEs.	Mention initiatives to counter LWEs	Conclude by emphasizing the need to combine strong security measures with inclusive governance and long-term development to achieve lasting peace.

2. THREATS TO INTERNAL SECURITY

2.1. TECHNOLOGY AND INTERNAL SECURITY

2.1.1. ONLINE RADICALISATION AT A GLANCE

Key factors behind radicalisation

Push Factors
- **Economic:** Unemployment, poverty
- **Social:** Marginalization, discrimination
- **Political:** Loss of faith in political institutions

Pull Factors (Attracting Forces)
- **Monetary Incentives**
- **Online Propaganda**
- **Exploiting Crises:** e.g., Israel-Gaza conflict

Factors facilitating online radicalisation

Echo Chamber	Micro-Targeting & Profiling	Cybercrime as a Tool	Terror Financing
Social media creates echo chambers that amplify extremist narratives.	Collected user data is used to psychologically influence vulnerable individuals.	Radical groups exploit digital frauds to finance operations and recruit members.	Online platforms help raise funds through anonymous campaigns.

Challenges in tackling online radicalisation

Easy Digital Access	Anonymity & Secrecy	Psychological Manipulation	Legal Gaps
Growing internet reach increases exposure to extremist content (~67% global population is online).	Encrypted apps and the Dark Web make detection and tracking difficult.	For example, **algorithms radicalization** traps users in narrow, biased viewpoints (rabbit holes)	No universal definition of radicalisation or terrorism hampers coordination.

Key Initiatives that could facilitate curbing online radicalisation

India
- **Statutory:** IT Act 2000 allows blocking harmful content.
- **Institutional:** I4C & MeitY Monitor and block URLs threatening national security.
- **Awareness Campaigns:** Sahi Raasta and Operation SADBHAVANA by Indian Army; Operation Pigeon by Kerala government to de-radicalize youth.

Global
- **Tech Against Terrorism:** Supports governments and tech firms in removing terrorist content online.
- **Christchurch Call:** Promotes a safer internet by countering extremist content.
- **INTERPOL:** CBI (as INTERPOL's NCB) leads India's coordination and also launched Bharatpol to boost global cooperation.

Way forward to tackle online radicalisation

Build Counter-Narratives	Ensure Accountability	Rehabilitation Support	Enhance Global Cooperation
Run awareness campaigns to **debunk fake news** and **break echo chambers.**	**Ensure Accountability:** E.g., **Germany's Netz** law fines social media platforms (with large user) for not removing harmful posts quickly	**Rehabilitation Support victims** of terrorism through better rights and rehabilitation.	Foster **international collaboration** between law enforcement and intelligence agencies.

2.1.2. SOCIAL MEDIA INFLUENCERS' AND NATIONAL SECURITY

Why in the News?

A YouTube vlogger/influencer from Haryana, has been arrested on charges of espionage.

More on the News

- The Social Media influencer was booked under **the Official Secrets Act** of 1923 and **Section 152 of the Bharatiya Nyaya Sanhita (BNS)**
  - **OSA is a framework for dealing with espionage, sedition**, and other potential threats to the integrity of the nation.
    - **Section 22 of the RTI Act of 2005 grants its precedence over the OSA** of 1923 and any other legislation or document in force at the time.
  - **Section 152 of the BNS** deals with 'Act endangering sovereignty, unity and integrity of India.'

Social Media Influencers as a Threat to National Security

- **Psychological Warfare:** Spread **fake news and foreign narratives to shape public opinion.**
  - **E.g.,** China uses influencers to spread its official views and deflect **global criticism** over **Uyghur issues.**
- **Espionage:** May share sensitive information to enemy country (e.g., **Jyoti Malhotra** was allegedly recruited by the Pakistan intelligence agency).
- **Polarisation & Communal Tensions:** They can spread fake news and hate speech, inciting violence (e.g., over 1,000 accounts accused of inciting violence in Murshidabad in West Bengal blocked by Union Government).
- **Secessionist Agenda:** May promote separatist content (e.g., pro-Khalistani accounts like **Sikhs For Justice**).
- **Terror Propaganda:** Extremists use **influencers to radicalize youth** (e.g., Al-Qaeda's YouTube preacher Anwar al-Awlaki).

India's Steps to Counter Influencer-Driven Threats to National Security

- **Other Legal Framework**
  - **Information Technology Act, 2000 (IT Act): Section 69A** of the Act grants the government **power to block online content** in the interest of national security, public order, or sovereignty.
  - **IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**: Requires platforms **to appoint grievance officers, remove unlawful content within 36 hours**, and trace message originators upon government request.
- **PIB Fact Check Unit (FCU):** Notified to tackle **fake news**.

Conclusion

India's multi-layered approach combines existing OSA with modern IT regulations, creating a comprehensive framework that addresses both traditional espionage and contemporary digital threats through influencer networks.

2.1.3. CRYPTO CURRENCY HAWALA NEXUS

Why in the News?

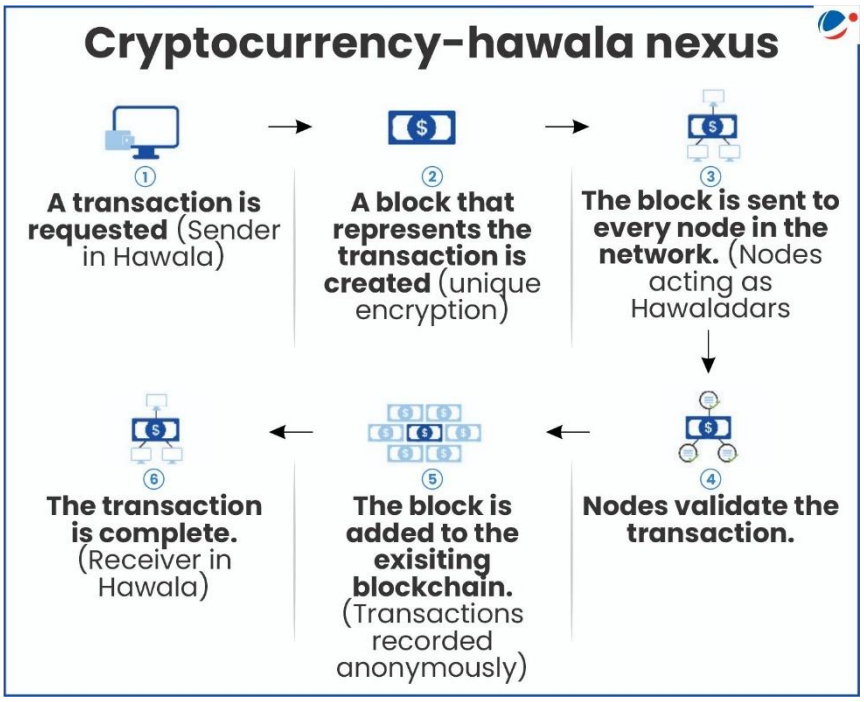
Supreme Court observed that **Bitcoin trading resembles a refined form of hawala .**

More on the News

- Supreme court also highlighted the **absence of a clear regulatory framework** for virtual currencies in India.
- Earlier in 2020, the Supreme Court in a landmark judgment quashed the **RBI's 2018 circular** prohibiting banks from offering services for virtual currencies.

About Cryptocurrency and Hawala System

- **Crypto Currency:**
  - It is any form of **currency that exists digitally or virtually and uses cryptography** to secure transactions.
  - Bitcoin is the most popular example.
- **Hawala System**
  - It is an **informal money transfer system** using agents called **hawaladars.**
  - It is **often linked to money laundering and terror financing.**
- **Cryptocurrency-Hawala Nexus**
  - It refers to the **convergence of traditional** hawala and modern **cryptocurrency**, for creating a potent channel for **laundering illicit funds** and **bypassing formal financial regulations**.
  - In blockchain, **nodes may be seen as analogous to hawaladars**, as both rely on **mutual trust or consensus** to sustain the integrity of their respective networks (see infographic).



Concerns of the Cryptocurrency Hawala Nexus

- **Enables Illicit Use**: Their secrecy helps in money laundering, terror financing, and tax evasion.
  - **Avoid Traditional Banking:** Operate outside regular banks, **useful in** unstable regions or where financial rules are tight.
  - **Hard to Trace:** Cryptocurrencies often use **stealth addresses** and ring signatures (e.g., Monero) or zk-SNARKs (Zcash) to obscure transaction. Example, Hamas used crypto to raise operational funds.
- **Global Reach: Hawala via Blockchain** adds **speed, trust, and global scale** to hawala through smart contracts.
- **Regulatory Gaps**: India's current laws don't clearly address crypto transactions or blockchain, creating a legal grey zone.

Way Forward to Tackle Crypto-Hawala Nexus

- **Global Cooperation:** International coordination is vital for tracking illicit crypto flows. **Example: UN Global Programme against Money Laundering**.
- **Tech-Driven Compliance**: Tools like **blockchain analytics** and platforms such as VTAC (**value-driven-Transactional tracking Analytics)** and TRM Labs help monitor fund usage.
- **Stronger Regulations:** Clear laws on virtual currencies are essential**. FATF guidelines and EU's MiCA** offer strong models for AML/CFT (Anti-Money Laundering and Combating the Financing of Terrorism)
- **Holistic Strategy**: Combating this nexus requires strict laws, anti-money laundering efforts, and technologies like **AI and machine learning**.

Conclusion

The Supreme Court's link between Bitcoin and hawala underscores rising risks from crypto-driven illicit finance. India needs clear laws, tech tools, and global cooperation to protect financial and national security.

2.1.4. ROLE OF QUANTUM COMPUTING IN NATIONAL SECURITY

Why in the news?

NITI Aayog's Frontier Tech Hub released a paper on **"Quantum Computing: National Security Implications & Strategic Preparedness".**

About Quantum computing:

- Quantum Computing is an emerging field of computer science that **uses quantum mechanics** to solve problems beyond the capabilities of classical computers.
- **Qubits are the fundamental building blocks of quantum computers**, and their stability is crucial for harnessing quantum states for computation

How Quantum Computing is Reshaping National Security?

- **Cryptography and Cybersecurity**: Quantum computer could break widely used public-key encryption algorithms, rendering modern **internet security, online banking, and secure communications obsolete.**
- **Smarter Intelligence & Surveillance**: It would enhance **signals intelligence (SIGINT),** allowing nations to intercept, analyze, and decode communications at an unprecedented scale
- **Military Tech:** Quantum algorithms will **optimize logistics, resource allocation, and battlefield strategy**. Quantum-enabled AI (Quantum AI) will power autonomous military drones and robotic systems,
- **Economic Warfare:** The ability to break current encryption could **destabilize financial markets, compromise banking systems, facilitates stealing intellectual property.**
- **Geopolitical Power:** Early leaders in quantum tech will dominate future global power dynamics. E.g., **China's Micius satellite (2016**) enabled secure quantum communication.

Key Steps taken by India in Quantum Technology

- **National Quantum Mission:** Boosts R&D and builds a strong quantum tech ecosystem.
- **QuEST (Quantum-Enabled Science and Technology)Program** : DST-led funding for quantum labs and infrastructure.
- **Academic Hubs**:
  - **IISc Bangalore**: Focus on algorithms and error correction.
  - **IIT Madras**: Centre for Quantum Computing (CQuICC).
- **Startups**: QNu Labs (under NQM) is building the world's **first quantum-safe network**.
- C-DOT's **Quantum Lab in Delhi and indigenous Quantum Key Distribution (QKD) system.**

Key Recommendations For Leveraging Quantum Computing for National Security

- **Develop Post-Quantum Cryptography (PQC):** Create a risk-based plan with fast testing, certification, and info-sharing for PQC (algorithms designed to resist quantum attacks).
- **Continuous Monitoring:** Set up a dedicated **quantum task force** to track global tech progress and adversarial capabilities.
- **Global Collaboration**: Partner with like-minded nations to advance QIS/E.g. India-EU agreement (2022) on quantum tech and HPC.
- **Other Steps:** Develop a **crypto agility framework** to quickly adapt encryption, ensure **flexible R&D funding** based on tech progress.

Conclusion

With its transformative potential across defense, intelligence, and secure communications, quantum computing will be a cornerstone in India's journey toward strategic resilience and the **vision of Viksit Bharat by 2047.**

2.2. DATA PROTECTION AT A GLANCE

Data Protection

- **Data Protection** is the process of **safeguarding important data from corruption, compromise or loss.**
- **Data** refers to **unprocessed facts and figures** which could be **'personal' or 'non-personal'.**

Relevance of data usage

Political Accountability	Efficient Administration	National security
Can improve transparency in governance by real time monitoring	Helps in making targeted and tailored programmes **(E.g. UIDAI)**	**NATGRID** for unified intelligence database and **DNA Databanks** for both criminal and civil matters

Need for protecting data

Enforcing Right to **Privacy under Article 21 of the Constitution (Puttaswamy Vs UoI**, 2017).	**Digitalisation of Economy** India's Digital Economy Is Expected to contribute nearly **1/5th of national income by 2029-30**	**Fortify digital governance** Quality data powers efficient digital platforms, such as UPI and Aadhaar	**Build Public Trust** Protect Critical infrastructure, prevent cyber financial frauds, etc,

Challenges in data protection

Techno-colonialism More than 80% of India's data is exported to global data centers	**Cyber security Risk** India Cyber Threat Report 2025 uncovered around **369 million distinct malware detections**	**Data Localization Challenges** challenges in ensuring secure storage and management of data within India.	**Other Issues** Suboptimal funding for research & innovations, low awareness about data privacy, disparities in Digital Literacy, etc.

Steps taken for data protection

Digital Personal Data Protection Act (DPDP), 2023 **Based on BN Sri Krishna Committee,** establishes principles for the **collection, storage, processing, and transfer of personal data.**	**IT Rules, 2021 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021** cast specific legal obligations on intermediaries, and platforms to ensure their accountability towards safe and trusted internet	**Cyber Surakshit Bharat Program** For enhancing cybersecurity awareness and capacity across the nation	**Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA)** Launched under the Digital India initiative for promoting Rural Digital Literacy

Ways to Further Strengthen Data Protection

Enhance Digital sovereignty Build **indigenous digital systems e.g.,** ONDC (Open Network for Digital Commerce), India Stack.	**Anonymization of personal data** Through techniques like Pseudonymization/ De-identification **(e.g. data masking)**	**Capacity Building** Effective **Professional Development Programs in Cybersecurity** for professionals across Government, Public Sector and Industry launched by the CERT-In.	**Learning from Global Best Practices** For example, General Data Protection Regulation (GDPR), Digital Markets Act (DMA) protects the personal data and privacy of people

2.2.1. DIGITAL PERSONAL DATA PROTECTION ACT (DPDP), 2023

Why in the News?

MeitY released the **draft Digital Personal Data Protection Rules, 2025** to implement the **DPDP Act, 2023**.

Highlights of DPDP Rules 2025

- **Clear Notices:** Data fiduciaries must clearly inform individuals about data use.
- **Data Deletion:** Data fiduciaries must erase personal data if the data principal does not respond within the given time.
- **Cross-Border Rules:** Data fiduciaries must follow government norms for sending data abroad.

About Digital Personal Data Protection Act, 2023

It was enacted to establish a comprehensive framework for **Protection and Processing of Personal Data.** Its key fatures are as follows:

Specifications	Detail
Applicability	• Covers processing of **digital personal data collected in India** or digitized later, and data processed abroad for offering goods or services in India. • **Excludes data processed for personal use or publicly available data** shared by the data principal or by law.
Consent	• Data requires the data **principal's consen**t, **withdrawable anytime,** except for legitimate uses like **government services or emergencies**.
Data Protection Board of India (DPBI)	• Established by the **Central Government**, it monitors compliance, imposes penalties, manages data breaches, and resolves grievances.
Rights and Duties of Data Principal	• Rights include access to data processing info, **correction, erasure, grievance redressal, and nominating representatives.** • **Must avoid false complaints**; violations can incur penalties up to Rs 10,000**.**
Obligations of Data Fiduciaries	• Ensure **data accuracy and security.** • **Inform** DPBI and affected persons **if breaches occur.** • **Erase data when no longer needed** or legally required**.**
Significant Data Fiduciaries (SDF)	• Notified by the **government for high-risk data processing**, they must appoint data protection officers, auditors, and conduct impact assessments.
Parental Consent	• Parental consent is required for **processing children's data** (under 18), with harmful data use and targeted ads banned.
Exemptions	• **Security agencies, research, startups, law enforcement**, etc. are exempted.

Issues of DPDP Act:

- **Privacy Risks**: State exemptions may lead to excessive data collection, risking the fundamental **right to privacy.**
- **Missing Rights**: The Act lacks the right to **data portability** (transfer data for personal use) and the **right to be forgotten**.
- **Cross-Border Transfers**: Allows mostly unrestricted data transfer, with **few country restrictions.**
- **Harm Regulation**: Doesn't address risks like **identity theft**, **financial loss**, or discrimination.
- **Board Independence**: Two-year terms with reappointment may reduce the Data Protection Board's independence **compared to regulators like SEBI and CCI, which have five-year terms.**

Way Forward

- **Adopt Global Best Practices:** Draw from **international models like the EU-US Data Privacy Framework** to enable secure cross-border data flows.

- **Encourage Bilateral Agreements:** Facilitate secure data transfers through international agreements, avoiding rigid isolationist mandates.
- **Regulatory Adaptability:** Continuously update frameworks for new privacy risks and technologies by creating a dedicated **AI-Privacy task force** to identify risks and develop adaptive regulations.
- **Clear definition:** Clearly define terms like "**sovereignty**" and "**integrity of India**" and set a clear process for granting exemptions.

Conclusion:

The 2025 draft rules are a key step in implementing the DPDP Act, 2023, by defining data fiduciary duties and protecting individual rights. To strengthen India's data framework, gaps like broad state exemptions and missing rights must be addressed, with focus on global best practices and regulatory clarity.

2.2.2. FACIAL RECOGNITION TECHNOLOGY

Why in the news?

NITI Aayog's White Paper on **Responsible AI for All** explores Facial Recognition Technology (FRT) as its first use case, aiming to build a framework for its **safe and responsible use** in India.

About Facial Recognition Technology (FRT)

It is an AI system that **identifies a person** using images or video **through complex algorithms.**

Key Applications of FRT

Security-Related Uses	Non-Security Uses
• **Law Enforcement:** Identifies suspects and criminals (e.g., **UP's Trinetra** system). • **Crowd Monitoring:** Tracks suspicious activity during events and protests. • **Missing Persons:** Helps trace and reunite missing individuals.	• **Identity Verification:** Aadhaar-based services, welfare schemes like **Take Home Ration**. • **Contactless Services:** Digi Yatra for airport entry. • **Education Access:** CBSE's face-matching for academic documents.

What are the risks associated with FRT systems?

- **Bias and Misidentification**: FRT often shows errors, especially for **women, darker skin tones, and minorities**. Many imported systems do not reflect **India's diversity**.
- **Privacy and Security Threats**: Facial data is sensitive and can be **hacked** or **misused**, leading to **privacy breaches**.
  - According to the **Puttaswamy Case 2017**, using data without consent or for unrelated purposes can **violate the right to privacy**.
- **Lack of Accountability**: Too many actors involved in FRT systems make it **hard to fix responsibility**.

Key Recommendations of NITI Aayog for responsible use of FRT

- **Privacy & Security**: Ensure legality, reasonability, and proportionality.
  - Example: Digital Personal Data Protection Act, 2023
- **Governance Framework**: Define liabilities for harm caused by FRT.
- **Privacy by Design**: Obtain explicit user consent.
- **Accountability**: Promote transparency, address algorithmic bias, and set up grievance redressal.
- **Safety & Reliability**: Publish standards on explainability and error rates.
- **Ethical Oversight**: Form ethics committee to review and guide FRT use.

Conclusion

Going forward, clear laws, transparency, and ethical use rooted in democratic values are essential to ensure FRT benefits society while protecting rights and reducing risks.

2.3. CYBER SECURITY AT A GLANCE

Cybersecurity

- Cybersecurity is the **convergence of people, processes, and technology** that combine **to protect** organizations, individuals, or networks **from digital attacks.**

Need for Cyber Security

Weopanisation of Internet Internet used for terrorist recruitment and funding (67% of the world population is online, India has the second-largest internet user base)	**Cyberspace Warfare** It can **disable official websites and networks,** disrupt or disable essential services, steal or alter classified data, cripple financial systems etc.	**Emerging technologies** Advanced technology like AL ,ML etc, are dual use technologies (Military & Civil) and their rising use in economy could also threaten internal security.	**Protecting Vulnerable Section** To combat **online Child Sexual Abuse** Materials, to contain trolling of women, etc. by predators exploiting anonymity

Existing Mechanism for Cyber Security

Joint Doctrine for Cyberspace Operations (2024): Emphasis on military aspects of cyberspace operations	**Policy initiatives** **National Cyber Security Policy (NCSP)** for building a resilient cyberspace and **National Digital Communication Policy, 2018** for resilient, and affordable Digital Communications Infrastructure.	**Other Measures:** IT Act 2000 (amendment in 2008), CERT-In. Defence Cyber Agency (DCA), **National Critical Information Infrastructure Protection Centre (NCIIPC),** Exercise Cyber Suraksha, etc.	**Global** **UN Convention on Cybercrime** is the **first legally binding global treaty** on cybercrime.

Challenges to Cyber Security in India

Transboundary Absence of any geographical constraints	**Finance** Huge investment is required to cope up with **rapidly evolving technologies**	**Policy issues** **Lack of national level comprehensive architecture for cyber security** like **Singapore model**	**Data colonialism** Overseas custody of data exposes the sensitive information of citizens to foreign attacks

Way forward

Data localization for better cyber security in line with **Justice B. N. Srikrishna Committee Report.**	**Setting up of Information Sharing and Analysis Centres (ISACs)** for information sharing and coordination in critical sectors	**PPP Model for Cybersecurity** to fill financial gap and facilitate capacity building.	**Learning from best practices** like **Tallinn Manual** 2.0 **of US**	**Upgrading cyber labs (E.g., CyPAD Initiative of Delhi)**

2.3.1. UNITED NATIONS CONVENTION ON CYBERCRIME

Why in the News?

The UN General Assembly adopted the **first legally binding global treaty on cybercrime**—the **UN Convention on Cybercrime**.

About The UN Convention on Cybercrime

- **Objective:** To provide **technical support** especially in developing countries **to prevent and combat cybercrime.**

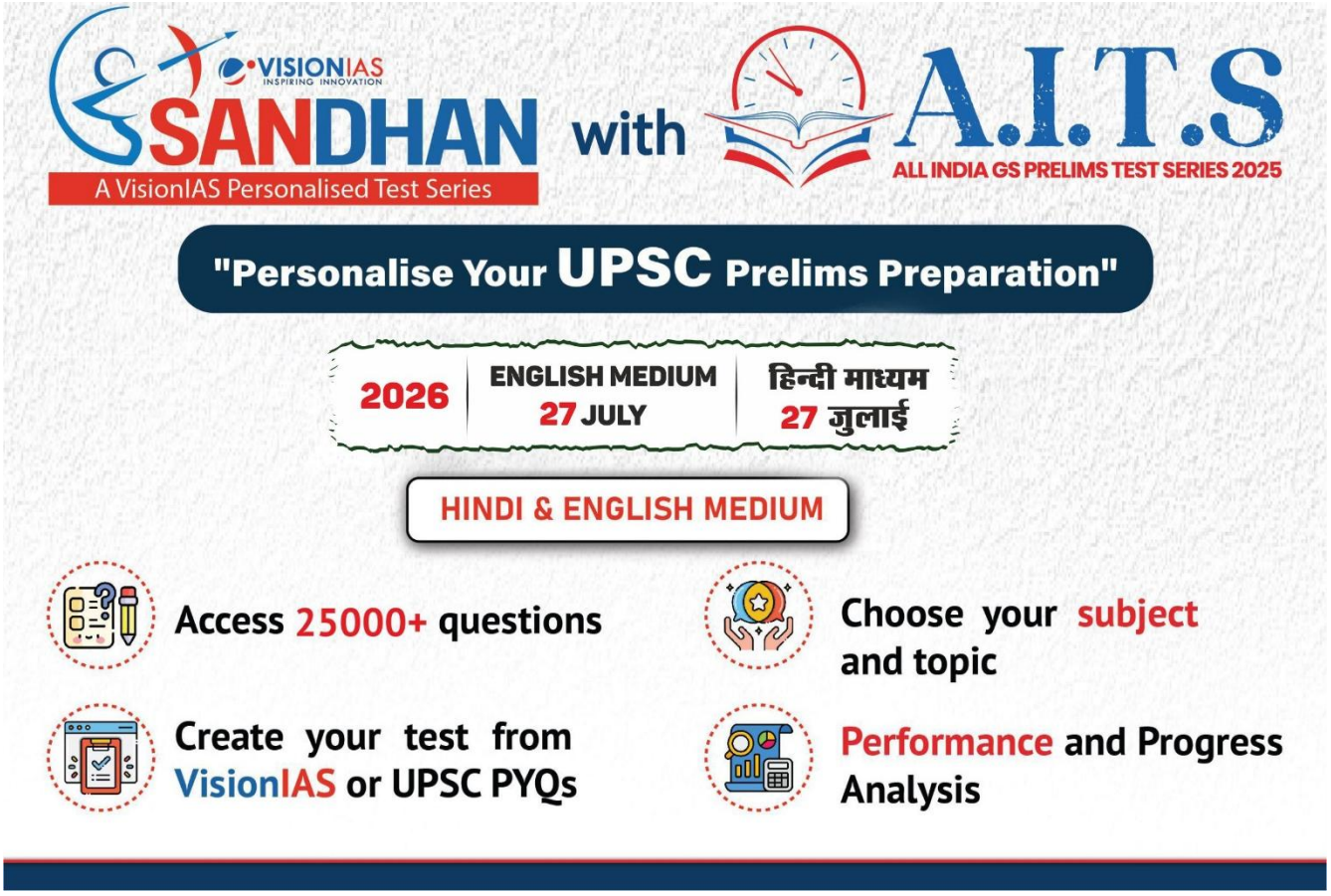
- **Key Provisions**
  - **International Cooperation:** Mutual legal aid, extradition, 24/7 assistance network, and asset confiscation cooperation.
  - **Procedural Measures**: Guidelines for preserving, searching, and seizing electronic data.
  - **Data Protection**: Compliance with privacy laws and safeguards for data transfer.
  - **Human Rights**: Ensures rights and freedoms are protected during enforcement.
  - **Criminalization of Key Offences:** Mandates State Parties to Criminalize offences like unauthorized access to **information system**, Child sexual abuse content, and Money laundering from cybercrime
  - **Others Provisions**: Joint investigations**, protection of victims and witnesses, etc.**

Need of the Convention

- **Growing Cyber Threats**: With **67% of the world online**, cybercrimes are rising—especially in **Southeast Asia**, affecting economies and infrastructure.
- **Cross-Border Investigations**: Cybercrimes often involve **evidence spread across countries**. The Convention supports **fast, secure international data sharing**.
- **Global Nature of Crime**: Criminals can **target victims in other countries**, making **global cooperation** essential.
- **Fast-Paced Tech Evolution and Penetration**: New tech like **AI and 3D printing** evolves rapidly. Policymakers struggle to **keep laws updated** (e.g., ChatGPT reached 100 million users in just 2 months)
- **Protecting Vulnerable Section:** Need to combat online abuse by predators exploiting anonymity on social media and games.

Conclusion

The UN General Assembly's adoption of the first criminal justice treaty in 20 years highlights successful multilateral cooperation and global commitment to combating cybercrime.



2.3.2. CRITICAL INFORMATION INFRASTRUCTURE AT A GLANCE

Critical Information Infrastructure (CII)

- The IT Act of 2000 defines "Critical Information Infrastructure" as a "**computer resource, the incapacitation or destruction of which shall have debilitating impact on national security, economy, public health or safety".**
- It primarily comprises the power, banking, telecom, transport, and government sectors.

Threat to Critical Information Infrastructure

State-Sponsored Cyber Attack	IoT Risk	AI in Cybersecurity	Mobile Security Threats
Target critical sectors like energy, banking, telecom; aim for espionage and disruption.	Widespread IoT use in smart grids and smart cities increases exposure	AI/ML used by both attackers (e.g. **automated phishing**) and defenders (e.g. **threat prediction**, **incident response**).	Mobile devices in CII sectors are targets for malware, spyware, and Wi-Fi attacks.

Challenges in Protecting Critical Infrastructure in India

India **lacks indigenization** in hardware and software cyber security tools like advanced firewall, cloud security etc.	**Inhibition** in private and public sector to **share information** about vulnerability of their systems.	Many organizations do **not have enough trained security professionals**.	Adapting to evolving laws (e.g. **Personal Data Protection Bill**, **IT Act**) is challenging

Steps Taken for Critical Infrastructure protection in India

Legislative measures	Institutional Measures	'Cyber Suraksha' exercise
National Cyber Security Strategy 2020, National Cyber Security Policy, 2013, Information Technology Act, 2000.	National Critical Information Infrastructure Protection Centre (NCIIPC), **I4C**, CERT-In, ,National Cyber Coordination Centre (NCCC).	Conducted by Defence Cyber Agency to simulate real-world cyber threats, reinforce secure practices

Way Forward to Protect Critical Infrastructure in India

Comprehensive Security Approach	Strengthen Cyber Intelligence	Public Private Partnership	Learn from Global Best Practices
Focus on identifying vulnerabilities and interdependencies across sectors.	Adopt modern tools like the **Cyber Kill Chain** to trace and respond to attack stages effectively.	sector to enhance research funding and innovation for protection and response mechanisms.	India should formulate international norms for CII protection, inspired by **Australia's Critical Infrastructure Resilience Strategy.**

2.4. GEOSPATIAL DATA AND NATIONAL SECURITY AT A GLANCE

Geospatial Data

- **Geospatial data** refers to any data related to any features and phenomenon related to Earth and has **location as one of its attributes. It provides 3 types of information-** Location, Attribute, Temporal
- It is captured using technologies such as **LIDAR, RADAR, satellites, and photogrammetry.**

Significance of Geospatial Data in National Security

Enhancing precision and reliability of **intelligence, surveillance**, via GPS	**Advancing situational awareness and Maritime Domain Awareness.** E.g. UAVs for search and rescue operations	**Supporting military operation** in logistics management, developing tactical plans,etc.	**Tackling new and emerging threats** like cyber –attacks, hybrid warfare, etc.	**Modernizing security operation** e.g., Crime prediction and precision guided munitions

Steps taken by India to develop its Geospatial Capabilities

Strengthening Policy Framework National Geospatial Policy, 2022 and National Map Policy	**Institutional Development** Creation of specialised bodies like the **Indian Institute of Remote Sensing**.	**Educational and Research Activities National Centre for Geodesy (NCG)** has been established at IIT, Kanpur	**Advancing Satellite Capabilities** Building a network of Earth Observation Satellites (EOS) like **EOS-07** **NAVIC** (India's own satellite-based navigation system).	**Developing Spatial Data Infrastructure** Platforms like **Bharatmaps** and **Bhuvan** support data sharing and access. Programs like **PM Gati Shakti** and **SVAMITVA** aid in large-scale geospatial data gathering.

Challenges in leveraging Geospatial Data for National Security

Skill and Data Accessibility Gaps › Shortage of experts to interpret geospatial data. › Limited access to high-resolution data.	**Research Funding** Insufficient funding for advanced geospatial technologies and analytics and scattered research	**Data Security Risks** Lack of secure systems to store sensitive geospatial data amid growing cyber threats. Weak locational privacy laws raise concerns over data misuse and surveillance.	**Inter-Governmental Coordination** Unclear rules on data sharing across central, state, and local levels.

Way forward to effectively leverage Geospatial Data for National Security

Foster Collaboration Build synergy between **government, academia, and industry** to boost innovation and efficiency.	**Promote Specialized Education** Encourage study in fields like **Geo-Informatics**, **big data analytics**, and **remote sensing** to build skilled professionals.	**Improve Inter-Agency Coordination** Enhance collaboration among **police, defence, and intelligence agencies** for better data use in national security.

2.5. MONEY LAUNDERING AND SMUGGLING

2.5.1. MONEY LAUNDERING AND TERRORIST FINANCING (ML/TF)

Why in the News?

Financial Action Task Force (FATF) released **"Comprehensive Update on Terrorist Financing Risks (2025).**

Key highlights of the report

- FATF acknowledges **state sponsorship of terrorism as a longstanding Terror Financing (TF) threat to global peace and security**
  - State sponsorship includes **direct funding, logistics, materials, or training.**
- India, in its National Risk Assessment (NRA) **for Money Laundering and Terrorist Financing 2022,** has identified **Pakistan's state sponsorship of terrorism as a TF source.**
  - India has declared **zero tolerance towards terror financing and money laundering**, working actively with FATF.

What is Money Laundering and Terrorist Financing (ML/TF)?

Money Laundering (ML)

- **Money Laundering** is the **process of making illegally-gained proceeds** appears legal.
- Money could be laundered through hawala, cryptocurrencies, shell companies, bulk cash smuggling, etc.
- Such money is used for **arms dealing, organized crime, terrorist financing, drug and sex trafficking**, etc

Terrorist Financing (TF)

- It encompasses the **means** used by terrorist organizations to finance their activities.
- It can come from both **legitimate** (i.e., profits from businesses and charitable organizations) and **criminal sources** (i.e., Drug trade, weapon smuggling, kidnapping for ransom).
- **Key methods**
  - **Online crowdfunding** disguised as charity.
  - **Microfinancing by lone actors**, often using small legitimate incomes.
  - **Gaming platforms** for streaming, donations, and recruitment.
  - **Decentralized financing**, often from regional hubs or self-financed cells.
  - Increasing threat from **tech-savvy youth** using social media and petty crimes.

Challenges in Tackling ML/TF

- **Weak enforcement**: 69% of countries show major gaps; ED's conviction rate under PMLA is just 4.6%.
- **Delayed trials** hamper timely action.
- **Virtual Digital Assets (VDAs)** allow anonymous, cross-border transfers.
- **Poor political will** and **tax havens** hinder global efforts.
- **Lack of inter-agency coordination**.

Initiatives taken to curb ML/TF

- **India**
  - **Statutory Measures:** Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015 (BMA, 2015), Prevention of Money Laundering Act, 2002 (PMLA),
  - **Institutional framework:** Directorate of Enforcement (ED) and Financial Intelligence Unit – India (FIU-IND).
  - **Taxing VDA:** Even tough in India crypto-assets are not legal tender, income from VDAs like cryptocurrencies is taxed at 30% and a 1% TDS is applied on crypto transactions to monitor and track usage.
- **Global**
  - Financial Action Task Force (FATF)

- UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention),
- Global Programme against Money Laundering.

Way Forward

- **Enforce FATF Standards** globally to close legal loopholes.
- **Tackle crypto havens** by regulating Virtual Assets and Service Providers (VASPs).
- **Capacity building**: Train national agencies to use tech and conduct financial investigations.
- **International Cooperation**: Support conventions like **Palermo Convention** (2000), **UNCAC** (2003).
- **Adopt Technology**: Use **AI and blockchain** for tracking and tracing funds.
- **Improve Coordination**: Regular data-sharing between banks, agencies, and global partners.

Conclusion

ML/TF continues to exploit weak links. A **strong, tech-enabled, and globally coordinated approach** involving both public and private sectors is essential to close these gaps.

2.5.2. FINANCIAL ACTION TASK FORCE (FATF)

Why in the News

FATF's report on **"Complex Proliferation Financing and Sanctions Evasion Schemes"** reveals new methods used to bypass global sanctions aimed at stopping proliferation financing.

Financial Action Task Force (FATF)

- **Genesis:** Established in 1989 during the G7 Summit in Paris,
- **Role:** Sets international standards that enable national authorities to effectively track and act against illicit funds linked to drug trafficking, the illicit arms trade, cyber fraud, and other serious crimes.
- **FATF Lists:** The FATF identifies **jurisdictions with weak measures** to counter money laundering, terrorist financing, and proliferation financing.
  - **Grey List:** Countries **working with the FATF to address strategic deficiencies** in their regimes
  - **Blacklist**: Countries or jurisdictions with **serious strategic deficiencies**
- **Members: 40-member (including India)**
- **Jurisdiction Scope:** FATF has led to more than 200 countries and jurisdictions committing to implement FATF's Standards, forming a **co-ordinated global response to prevent organised crime, corruption, and terrorism**.

What makes functioning of FATF less effective?

- **Perceived lack of objectivity:** FATF makes decisions by consensus, and **no formal rules exist** as to how many members must object to spare a country from inclusion in grey list.
- **Focus on Technical Compliance, Not Real Action:** Pakistan was removed from the FATF grey list after meeting technical requirements, even though it failed to take concrete action against terrorism and terror financing.
- **Weakness in Listing Regime**: Placing non-compliant countries either in black list or the grey list does not allow for a flexible and graduated response against terror financing countries.
- **Marginalisation of Global South voices:** many African countries appear to be regularly placed on and off the grey list as they lack resources (not intent) for compliance.
- **Emerging source of terror financing:** The rise of cryptocurrencies and other virtual assets have provided terrorists with new avenues to move funds anonymously and internationally.

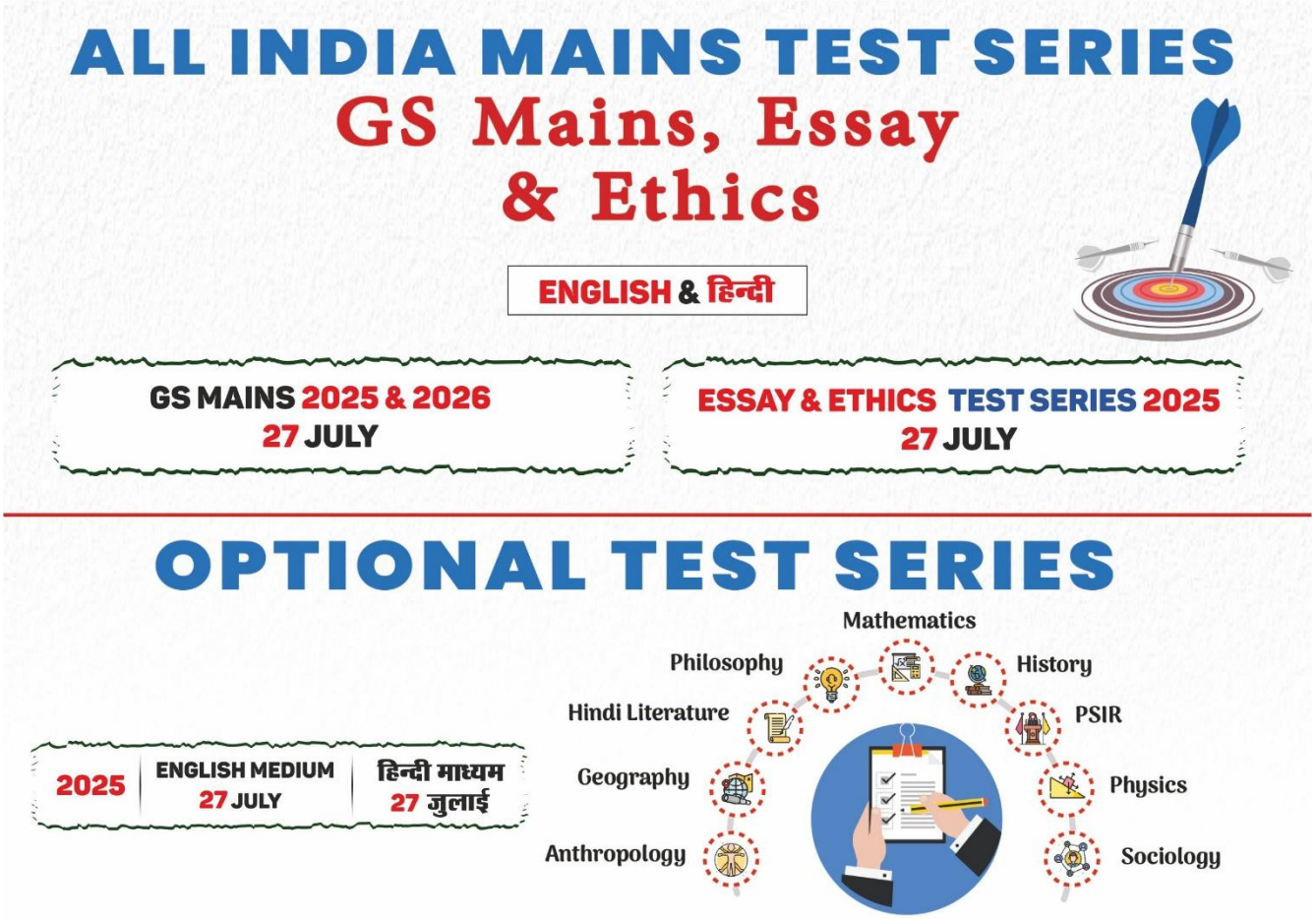
Way forward for making FATF more effective

- **Improve Transparency:** Ensure open and competitive appointments in the FATF secretariat. Secure job independence and stability for secretariat staff.

- **Categorisation within grey list**: Classify grey list countries based on willingness to comply for effective follow-ups.
- **Support for Poor Nations:** Offer special aid to countries needing help in improving legal, financial, and regulatory systems.
- **Build Capacity for Emerging Threats:** Update standards regularly to address new risks like virtual assets and cryptocurrency-based terror financing.
- **Boost Global Cooperation:** Collaborate with global bodies like the UN, IMF, World Bank, and regional FATF-style groups to strengthen impact.

Conclusion

An objective and transparent FATF is vital for global security, as it ensures credible action against money laundering and terror financing. Therefore, strengthening its processes, addressing emerging threats, and supporting weaker nations are essential.



2.5.3. DRUG TRAFFICKING IN INDIA AT A GLANCE

Drug Trafficking

Drug Trafficking is the illegal **production, distribution, and sale** of substances banned under drug laws. **292 million** people used drugs in 2022 — a **20% increase** in 10 years (World Drug Report 2024).

Key Issues Linked to Drug Trafficking

National Security Threat	Rising Social Crimes	Institutional Corruption	Environmental Damage
› Fuels crimes like **human trafficking** and **money laundering** › Leads to **narco-terrorism**, destabilising regions › Drug money funds **terrorism and LWE**	Increases **youth addiction**, affecting public health and law & order	Drug cartels infiltrate and corrupt state systems E.G., PUNJAB DRUG SCANDAL 2024	Illegal drug farming causes **deforestation** and increases **carbon footprint** E.g., Cannabis cultivation in Uttarakhand

Key challenges in tackling drug trafficking in India (INCB Report 2023)

Transit Hub	Cyber enabled trafficking	illegal online pharmacies
India is wedged between the **world's two largest areas of illicit opium production, Death/ Golden triangle** (Myanmar, Thailand and Laos) and **Death/Golden Crescent** (Afghanistan, Iran, and Pakistan).	Cyber-enabled drug markets, operating on the dark web and crypto-markets, are making illicit drugs more accessible than ever before	Proliferation of illegal online pharmacies poses a significant challenge to drug control efforts.

Measure taken by India to tackle drug trafficking

Statutory	Databases	Task Forces	Global Cooperation
› Narcotics Drugs and Psychotropic Substances Act, 1985. › NIA empowered fo**r narco-terrorism** since 2020	**SIMS and NIDAAN** (National Integrated Database on Arrested Narco-offenders) portals for drug offences/offenders	Anti-Narcotics Task Forces (ANTF) in states/UTs	› UN Single Convention on Narcotics Drugs 1961 › UN Convention against Corruption (UNCAC) and UNTOC

Way Forward

Accountability	Coordination	Leveraging Technology	Other
Create accountability rules for shipping, railways, and air cargo.	Information sharing among enforcement agencies	Control drug supply chain on internet by regulating crypto-currency markets.	**Stricter penalties** under NDPS, effective implementation of **Nasha Mukt Bharat Abhiyaan**, etc.

2.6. TERRORISM

2.6.1. TERRORISM IN INDIA AT A GLANCE

Terrorism In India

- India ranked 14th on Global Terrorism Index 2025 (Topped by Burkina Faso).

Challenges to counter International Terrorism

Definition Gap	State Sponsored	Emerging technology	Internal Factors	Ineffective global cooperation
No global consensus on definition of 'terrorism'.	Pakistan has supported terrorism through funding, **logistics, materials, and training** (2025 FATF report).	Use of **social media, crowdfunding,** Bitcoin to raise fund, presence of **Virtual Terror Groups etc.**	**Porous borders, AFSPA**-driven political alienation, support from **Over Ground Workers** (OGWs), **hybrid terrorists,** and **lone-wolf** radicals hidden in society.	Example, China vetoes terror listings (e.g., Masood Azhar at UNSC).

Counter terrorism Initiatives

India

- **New Security Doctrine (2025):** Zero tolerance for terrorists and their supporter
- **UAPA, 1967:** Legal framework to ban terrorist activities.
- **NIA:** Central agency to investigate terror cases.
- **NATGRID:** Database for real-time intelligence sharing.
- **Community participation:** Schemes like **HIMAYAT (skills), UMEED (women),** and promotion of tourism and crafts encourage local jobs.
- **Rehabilitation: Operation Sadbhavana** support former militants, orphans, and affected families.

Global

- **Financial Action Task Force (FATF):** Apex watchdog for Anti-Money Laundering and Countering the Financing of Terrorism.
- **UN Global Counter-Terrorism Strategy (2006):** Boosts global cooperation against terrorism.
- **UNSC Counter-Terrorism Committee (CTC):** Ensures countries follow anti-terror Resolution 1373 (2001).
- **Global Counterterrorism Forum (GCTF):** Multilateral anti-terror platform; India is a member.
- **SCO RATS:** Fights terrorism, extremism, and separatism in the region.
- **No Money for Terror Conference:** India hosted the 3rd conference in New Delhi to combat terror financing.

Way Ahead for tackling terrorism

Define Terrorism	Border Security	National Capacity Building	Strengthen Global Cooperation
adoption of **Comprehensive Convention on International Terrorism (CCIT)** at the UN proposed by India in 1996.	Speed up deployment of **smart fencing, thermal sensors,** and **surveillance** along the LoC (as per **Madhukar Gupta Committee).**	Strengthen intelligence agencies (R&AW, NIA), Balance **HUMINT** (Human Intelligence) with **TECHINT** (Tech Intelligence), **expand De-Radicalization Programs**	Transparency in decision making of FATF, follow global norms like **UNSC Delhi Declaration** on tech misuse by terrorists.

2.6.2. INDIA'S NEW SECURITY DOCTRINE

Why in the News?

After the success of Operation Sindoor, the Prime Minister outlined a **new security doctrine,** signalling a major shift in India's **counterterrorism strategy.**

Key changes in India's Security Doctrine

Pillar	Shift and Significance
Decisive Retaliation against any terrorist attack on India's own term	• India has **lowered its response threshold** against terrorist attacks, raising costs for terror supporters
No Tolerance for Nuclear Blackmail and India will carry out precise strikes on terrorist safe havens, if needed	• Clear break from past restraint—**self-defense comes first**.
No Distinction between Terror Sponsors and Terrorists and both will be treated them as one.	• **State-sponsored terrorism** is now seen as **an act of war** by the supporting state.

Other key aspects of Security Doctrine during Operation Sindoor

- **Deterrence by Punishment:** The punishment strategy deters Pakistan by threatening heavy damage after a terrorist attack, replacing the earlier "**deterrence by denial**" approach.
- **Economic Measures:** Economic measures like **suspending the Indus Water Treaty** are now part of India's strategic approach to address security without military escalation.
- **Geopolitical Signalling:** India sent several high-level all-party delegations abroad to share its anti-terrorism stance and build international pressure on Pakistan..
- **Strategic De-capacitation**: India targeted Pakistani airbases to disrupt the Pakistan Air Force's operations, preventing further **waves of escalation**.
- **Coordinated, Tech-Driven Response**: India's precise response used **advanced indigenous technology like drones**, layered air defense, and electronic warfare.
- **De-escalation Strategy**: India punishes terror hubs while **limiting full-scale conflict**, placing responsibility on Pakistan.

Conclusion

Operation Sindoor marks a turning point in India's military and geopolitical approach. It shows India's clear intent to retaliate against cross-border terrorism by striking terror hubs, stopping enemy responses, and avoiding full-scale war.

2.6.3. INDIA'S DIPLOMATIC OUTREACH AGAINST STATE SPONSORED TERRORISM

Why in the news?

India dispatched high-level **multi-party delegations** to **more than 30 countries**, comprising **Members of Parliament from across political parties**

More on the News

Key Objectives of the outreach

- **Reframe the Kashmir Issue:** Present Kashmir as an **internal constitutional matter**, not a bilateral one.
- **Expose Terror as State Policy:** Show that Pakistan's use of terror is not just India's problem but a global threat to **international anti-terror norms.**

Effectiveness of India's Global Outreach Against State Sponsored Terrorism

- **Legitimizing Self-Defence:** India invoked **Article 51 of the UN Charter**, affirming its right to self-defence. This justified Operation Sindoor as a lawful response to **armed aggression.**
- **Zero-Tolerance Policy on Terror**: India stressed a firm, lawful stand against all forms of terrorism and urged the UN to adopt the **Comprehensive Convention on International Terrorism (CCIT).**
- **Building Global Support:** Example: **Colombia retracted its earlier statement** and reaffirmed support for India's anti-terror stance.

- **Support from Muslim Majority Nations:** India framed the issue as a **fight against terrorism, not religion or bilateral conflict.**
  - Countries like **Indonesia, Egypt, and Bahrain blocked Pakistan's anti-India move** at the OIC (Organization of Islamic Cooperation).
- **Global Standing:** Enhances India's global standing as a **responsible leader** and strengthens its role in shaping **international counter-terrorism efforts**.

Key Hurdles in India's Diplomatic Outreach Against State Sponsored Terrorism

- **Re-hyphenation of India and Pakistan**: Global focus is shifting back to **re-hyphenating** India and Pakistan as equal parties, **especially on Kashmir.**
  - It was **reinforced by US President Trump's claim of mediating** the ceasefire during Operation Sindoor.
- **Lack of Global Coordination**: **No coordinated sanctions or resolutions** have been imposed on Pakistan for its support of terrorism.
- **Pakistan's Global Gains**: Backed by China, Pakistan leads key **UN committees** (Chair of the UNSC Taliban Sanctions Committee and Vice-Chair of the Counter-Terrorism Committee) making it harder for India to press its case.
- **Continued Economic Aid to Pakistan:** Despite terror links, Pakistan still gets **financial support from IMF, World Bank, and ADB**, preventing effective isolation.
- **Short Global Focus**: Major crises like Russia-Ukraine, Israel-Hamas, and Iran tensions distract the world, allowing Pakistan to **regain influence** during these distractions.

Conclusion

India's firm stand on its security shows **strategic maturity**. The world values clear positions over compromise. Future conflicts will be won in **perception**, not just on the ground. **India must not only win battles but also shape the narrative**

2.6.4. TRANSNATIONAL ORGANISED CRIMES AT A GLANCE

Transnational Organized Crimes (TNOCs)

- **Organized crimes** are **illegal activities, conducted by groups or networks** acting in **concert** for a financial or material benefit
- **Transnational Organized Crimes (TNOCs) operates across borders**, exploiting vulnerable people and undermining global security.

Types of TNOC

Drug trafficking	**Human trafficking**	**Smuggling of migrants**	**Money laundering**	**Illicit trading in firearms**	**Crimes that affect the environment**	**Cybercrime**

Challenges in curbing TNOCs

Cross-Border Complexity TNOCs span **multiple countries**, making **law enforcement and jurisdiction** difficult.	**Legal and Policy Gaps** **Different laws and systems** across countries hinder coordinated global action.	**Demographic Winter** Ageing populations in developed countries increase demand for **labor and fuels trafficking**.	**Economic Inequality** **Poverty and joblessness** drive vulnerable individuals toward **organized crime networks**.

Steps taken to address TNOCs

National

- **Constitutional and Statutory Framework: Article 23** of the Constitution and **Immoral Trafficking Prevention Act, 1956** prohibit human trafficking.
- **Maritime Security:** In 2022, India joined Combined Maritime Forces to fight illegal activities by non-state actors at sea.
- **National Central Bureau (NCB): CBI** acts as **India's National Central Bureau** for INTERPOL coordination.

Global

- **UN Conventions: UNTOC and its protocol against migrant smuggling (ratified by India) promote international cooperation.**
- **UN Commission on Crime Prevention and Criminal Justice (CCPCJ):** Main UN body for **crime prevention and justice policies**.
- **FATF**: Apex watchdog for Anti-Money Laundering and **Countering the Financing of Terrorism.**
- **INTERPOL** : INTERPOL's Organized Crime Unit and Project Millennium support tracking global crime networks.

Way Forward to Tackle TNOC

Secure Financial Systems Protect **markets and banking systems** from criminal networks.	**Enhance Law Enforcement** Provide **specialized training** and boost **intelligence capabilities**.	**Increase Accountability** Launch global initiatives to **hold countries accountable** for enabling organized crime.	**Focus on Rehabilitation** Reduce repeat offences through **rehabilitation and reintegration** of offenders.

2.7. EMERGING DIMENSIONS OF WARFARE

2.7.1. ADAPTIVE DEFENSE AND FRONTIER TECHNOLOGIES IN MODERN WARFARE

Why in News?

The Defence Minister stressed the need for an **'Adaptive Defense' strategy** to deal with fast-changing threats from **emerging and frontier technologies**.

What Are Frontier Technologies?

- They are fast-evolving innovations driven by **digitalization and connectivity.**
- **They could be:**
  - **Digital:** AI, IoT, Metaverse, Quantum
  - **Physical**: 3D printing
  - **Biological:** Bioprinting, genetic engineering

What is Adaptive Defense?

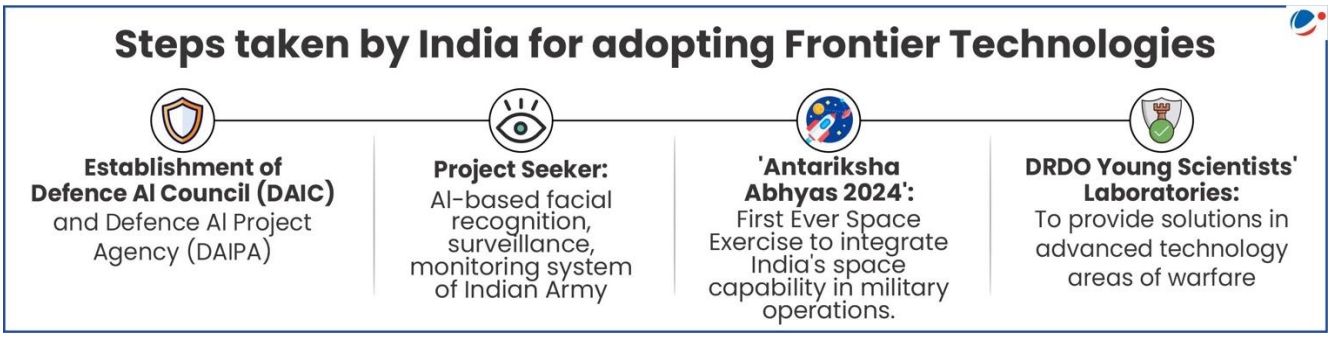
- **Definition**: A **strategic approach** where **defence systems evolve continuously** to counter emerging threats.
- **Core Principle**: Emphasizes a **proactive mindset** to anticipate, adapt, innovate, and respond effectively to unpredictable security challenges.
- **Key Capabilities**: **Situational awareness**, agility, resilience, **strategic flexibility**, and seamless integration with advanced technologies.
- **Significance**:
  - Secure the future beyond just protecting borders.
  - Designed to address both traditional (e.g., armed aggression) and non-traditional security challenges (e.g., Drug trafficking).
  - counter the menace of information warfare against national security, etc.

What are Key Technologies Reshaping Warfare?

- **Artificial Intelligence (AI**): Used in decision-making, target identification, and AI-powered drones.
- **Lethal Autonomous Weapon Systems (LAWS**): Operate without human intervention once activated.
- **Electromagnetic Warfare**: Manipulates electromagnetic spectrum for offensive and defensive operations.
- **Space Warfare**: Involves kinetic and non-kinetic attacks on space assets (**e.g. ASAT weapons**).
- **Information & Cyber Warfare**: Seeks dominance in the information domain; e.g. cybersecurity breaches like at **Kudankulam Nuclear Plant**.
- **Synthetic Biology**: Risks include illegal gene-editing, bio-hacking, and cyber-biological threats.
- **Laser & Electromagnetic Railguns:** Emerging tools for precise, high-speed attacks including on satellites

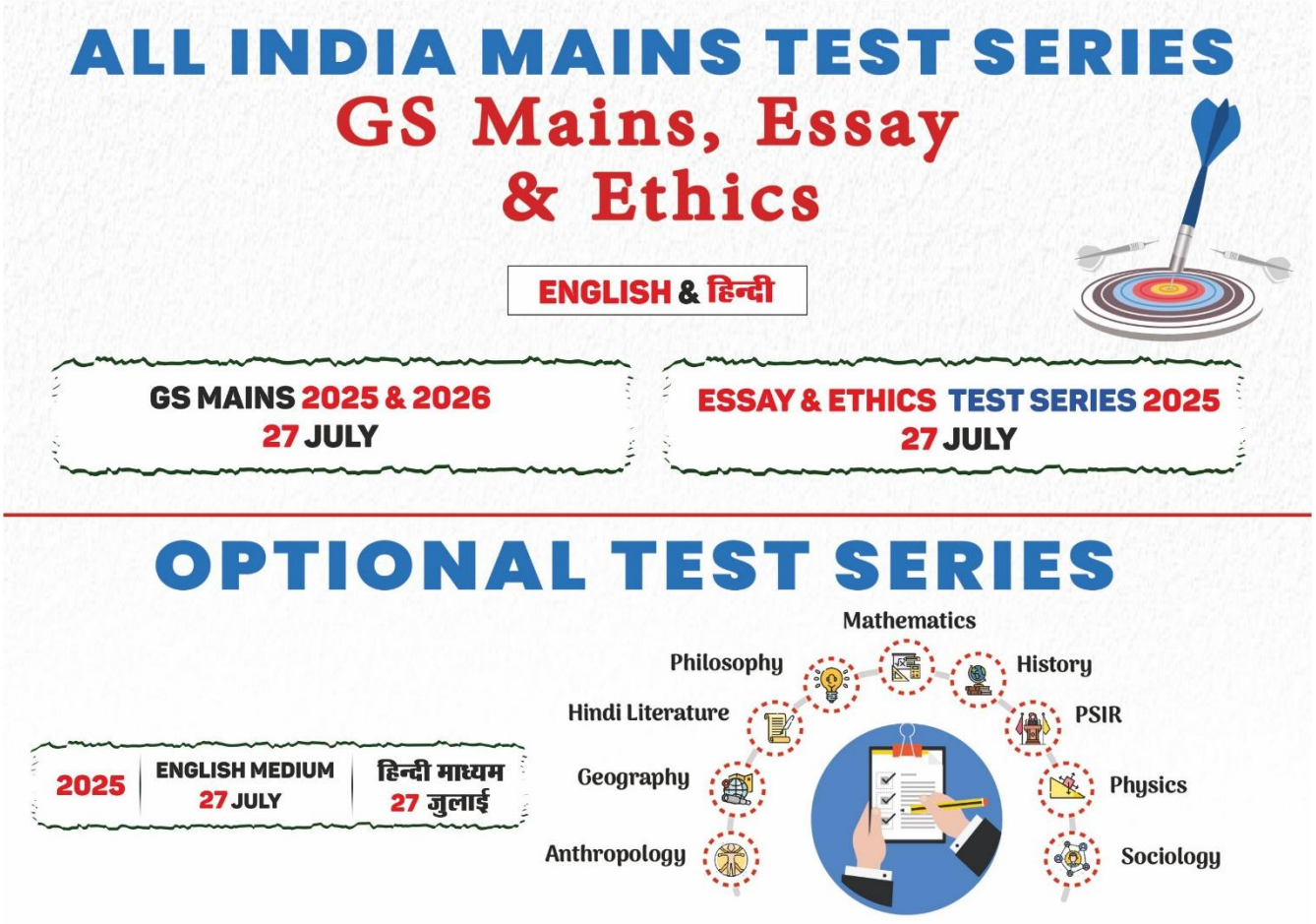
Challenges Posed by Frontier Technologies

- **Challenges to International Security:** Increased risk of **destabilization** due to asymmetry in technological capabilities and **proliferation of advanced technologies** to non-state actors**.**
- **Legal gaps:** lack **of international laws** on use of these technologies in warfare further increases vulnerability of **human rights violation**.
- **Dual use dilemma:** Technologies designed for **peaceful purposes** can be **repurposed** for military applications, blurring lines between civilian and military tech use.
- **Other Issues:** Risks of **algorithmic bias**, accountability issues, potential for AI arms races etc.



Conclusion

Adopting an **'Adaptive Defense'** strategy is imperative for India to secure itself in a rapidly transforming strategic landscape. Mastery of frontier technologies like AI, cyber, and space capabilities is not optional but essential.



2.7.2. HYBRID WARFARE AT A GLANCE

Hybrid Warfare

- **Hybrid Warfare** is a strategy that combines **conventional tactics (kinetic warfare)** with unconventional **methods (non-kinetic warfare)**, to achieve political or strategic goals without resorting to full-scale war.
- Hybrid warfare is a **tool used within the grey zone warfare (GZW).**
  - **GZW is** a broader concept involving **conflict tactics used between peace and full-scale war.**

Key characteristics of Hybrid Warfare

Blurred War-Peace Line	Ambiguity and Attribution	Multi-Domain Attacks	Use of Non-State Actors	Psychological Warfare (Info War)
Hard to tell when war begins, **making traditional responses ineffective.**	Attacks are vague and hard to trace, delaying response and accountability.	Involves land, air, sea, cyber, and space—making defence more complex.	Employs proxies and non-state groups to carry out operations.	Example: China renaming areas In Arunachal Pradesh to assert territorial claims.

Reasons for rise in Hybrid Warfare

Threat Assessment	Low-Cost	Ease of Attack	Lack of Global Rules
Hybrid threats are often missed by conventional security frameworks.	Cheaper than full-scale war and avoids direct blame. E.g., U.S. sanctions on Iran.	Cyber, AI, and digital tools make attacks easier. E.g., Russian cyberattacks on Ukraine.	No clear **international laws** to regulate grey-zone tactics, especially **cyber warfare**.

Factors making India vulnerable to Hybrid Warfare

Hostile Neighbours	Internal Unrest	Evolving Terror Tactics	Digitalisation of Economy
Pakistan and China supports **terrorism, fake currency, etc.**	Presence of **Left-Wing Extremism** and **ethnic tensions** in the Northeast.	Rise of **lone wolf attacks** and **sleeper cells**—hard to detect and prevent.	Threat of Cyber-attack on critical infrastructure (e.g. Possibility of Chinese malware attack on Mumbai power grid in 2021).

India's Hybrid Warfare Preparedness

Defence Modernisation	Structural Reforms	Global Partnerships	Parliamentary Oversight
Indigenous weapons like **DRDO's DURGA-II** Boost through **'Make in India'** in defence sector	Set up **CDS (Chief of Defence Staff)** Created **Defence AI Council** and **Defence AI Project Agency** for tech-led planning	**GSOMIA** with the U.S. **Quad cooperation** on cyber security and defence	**2024 Defence Committee** reviewing cyber defence, anti-drone tech, and system integration

Way ahead to combat Hybrid Warfare

Institutional Strengthening
- **Regular audits** of critical systems (e.g. fintech networks)
- **Create a Hybrid Warfare Division** for offensive and defensive action
- **Whole-of-Government Strategy** led by the National Security Council Secretariat

Real-Time and Tech-Based Response
- Train forces in **robots, drones, and smart tech**
- Use **real-time situational awareness tools** for quicker threat detection

Global Collaboration
- Promote **international cooperation** with clear rules and coordinated action for grey-zone threats

2.8. SPACE WEAPONIZATION AT A GLANCE

Space Weaponisation

- **Space Weaponisation** includes **placing weapons in outer space** as well as creating weapons that will destroy targets in space.
- It **is different from the militarization of space** that assists armies on the conventional battlefield.

Implications of space weaponisation

Fear of war	Threat to Peaceful Space Use	Space Debris Hazard	Risk to Critical Infrastructure
Increases chances of conflict, just like the **US–USSR space race** during the Cold War.	Hampers **scientific and commercial missions** like the Hubble Telescope and space research.	Over **40,500 debris objects** (larger than 10 cm) now orbit Earth, risking collisions (European Space Agency)	Weaponised space could target **Earth-based systems** like India's **IRNSS navigation satellites**.

Reasons behind space weaponisation

Gaining War Superiority	Protecting Satellites	Dual-Use Technology	Weak Space Treaties
Space control enhances dominance across **land, sea, air, and cyber warfare**.	Countries develop **ASAT (Anti-Satellite) weapons** to defend their space assets. Example: India's Mission Shakti	Many space tools like **GPS** have both **military and civilian uses,** making them strategic	Agreements like the **Outer Space Treaty (OST)** lack strict enforcement, leaving loopholes for weaponisation.

Key initiatives to prevent space weaponisation

Outer Space Treaty (1967)	PAROS (Prevention of an Arms Race in Outer Space)	Partial Test Ban Treaty (1963)	Artemis Accords
Promotes **peaceful use** of outer space. Prohibits placement of **nuclear weapons** or weapons of mass destruction in space.	UN initiative calling for a **ban on space weapons** (still under negotiation)	Bans **nuclear tests in space**, underwater, and the atmosphere. Aimed at **limiting space militarisation**.	Framework for **peaceful lunar exploration** and cooperation

Way forward to prevent space weaponisation

Space as a Global Commons	Legally-Binding Treaty	Space Domain Awareness	Transparency and Trust Building
Treat outer space ike **international waters**—used peacefully by all.	Enforce PAROS and make it legally binding	Boost monitoring systems (e.g., **Combined Space Operations Initiative**) to detect threats and manage debris.	Countries must **share accurate data** with the **UN Office for Outer Space Affairs (UNOOSA)** to build trust and reduce misunderstandings.

2.9. KEYWORDS

Keywords				
Eco-Chamber	Psychological profiling	Psychological Warfare	Secessionism	Post Quantum Cryptography
Intelligence & Surveillance	Right to be forgotten	Adaptive Defense	Kinetic warfare	Cyber terrorism
Situational Awareness	Golden Crescent	Golden Triangle	Hybrid Warfare	Lone Wolf Attack
Demographic Winter	Bio-hacking	Dual use dilemma	Algorithmic bias	Re-hyphenating

2.10. PRACTICE QUESTION

Answer Canvas

In the context of Operation Sindoor, critically examine the shift in India's counterterrorism doctrine and its implications for national security and regional stability?

Introduction	Body Part: 1	Body part: 2	Conclusion
Briefly introduce Operation Sindoor	Highlight Key Shifts in India's Security Doctrine	Implications of the New Doctrine. Further highlight some concerns	Conclude by stressing the need to balance decisive military action with diplomatic outreach, such as all-party global missions, to secure lasting national security and regional stability.

3. SECURITY CHALLENGES AND THEIR MANAGEMENT IN BORDER AREAS

3.1. SECURITY ISSUES IN BORDER AREAS

3.1.1. BORDER SECURITY AT A GLANCE

India and Bordering Countries

Implications of space weaponisation

Border	Challenges along Border	Initiatives taken
India-China	› **Border disputes** at Galwan Valley, Aksai Chin, Arunachal Pradesh, Doklam etc. › **Inadequate infrastructure** (access to rail, road etc.) due to high altitude terrain. › **Water- sharing issues** (e.g. Brahmaputra River).	› **Creating infrastructure** to reduce time for troop movement like Dhola- Sadiya Bridge. › **Development of North East Region.** E.g. Border Area Development Programme, **Vibrant Village programme** for border village development. › **Army infrastructure projects** within 100 km of LAC **exempted from forest clearance.**
India-Pakistan	› **Border dispute** at Sir Creek and Kashmir. › **Infiltration and Cross-border terrorism.** E.g. Uri ,pulwama and Pahalgam › Drones used for s**muggling arms and narcotics** across the border in Punjab › **Diverse terrain** including desert, marshes, snowcapped mountain and plains.	› **Comprehensive Integrated Border Management System (CIBMS)** To improve situational awareness at different levels of hierarchy. › **BIM (Border Infrastructure and Management) Scheme**: for developing infrastructure along India's international borders. › **Suspension of Indus water treaty (1960)**.
India-Nepal	› **Border dispute** at Kalapani, Limpiyadhura and Lipulekh. › **Fear of spread of Maoist insurgency** due to links of Nepal's Maoists in India. › **Easy escape & illegal activities like** drugs and arms smuggling, etc. › **Chinese investment in core sector of Nepal** like infrastructure, hydro energy, etc.	› Establishment of **Border District Coordination Committee.** › **Construction** of over 1300 km of roads along border. › **Development aid to Nepal.** (In FY 2024-25, India allocated Rs. 700 crore in aid to Nepal) › **Security related infrastructure development** like Fatehpur Border out Post.
India-Bhutan	› **Insurgency.** E.g. United Liberation Front of Asom (ULFA) camps in Bhutan. › **Smuggling of goods** like Bhutanese cannabis. › **Open Cross-Border Movement** led to human trafficking and smuggling of migrants.	› **Operation All Clear** by Royal Bhutan Army to remove insurgents camps in Bhutanese territory. › **Establishing new border posts in Sikkim.** › **General approval under Forest (Conservation) Act, 1980 for diversion of forest land** for infrastructure projects.
India-Myanmar	› **Drug trafficking** due to proximity to golden triangle. › **border** is **porous**, **poorly guarded**, and lies in a **remote, insurgency-prone area**.	› **Integrated Check Posts** to strengthen ties with **SAARC, Thailand, and Myanmar**. › **Operation Sunrise** targeting insurgents along the India-Myanmar border. › Proposal of fencing entire Indo-Myanmar border.
India-Bangla-desh	› **Illegal migration** into India (around 20 million as per 2016). › **Smuggling of goods** like jamdani sarees.	› **India-Bangladesh Land Boundary Agreement, 2015.** › Establishment of **Border Protection Grid (BPG).** › **BOLD-QIT** was implemented under the CIBMS scheme.

3.1.2. 25 YEARS OF KARGIL WAR

Why in the News?

India is celebrating 25 years of Kargil War victory.

About Kargil war

- The Kargil War broke out as **Pakistani troops secretly took over Indian Army posts that had been vacated for winter** to avoid casualties.
  - It **happened immediately after the 1999** Lahore Declaration which was aimed at easing nuclear tensions and resolve border issues peacefully.
- **Operation Vijay was launched to repel intruders** in Kargil and it was supported by airstrikes (**Operation Safed Sagar**) and naval action (**Op Talwar).**

Reasons for Kargil War

Politico-Strategic Motives	Military/Proxy War Related Motives
Internationalize Kashmir issue Alter the **Line of Control (LOC**) **Achieve a better bargaining position** for trade- off against the positions **held by India in Siachen**	**interdict the Srinagar-Leh road** by disrupting vital supplies to Leh Outflank Indian defences in **Turtuk and Siachen.** **boost militancy in J&K** by diverting troops from the Valley to Kargil.

Shortcomings in India's defense architecture that contributed to the Kargil War

Kargil Review Committee (KRC) led by **K. Subrahmanyam** identified key issues:

- **Intelligence failure**: Pakistan's intrusion was not anticipated, partly due to overreliance on the Lahore Declaration.
- **Low technology**: Lack of high-resolution satellite imagery, UAVs, and strong human intelligence delayed detection.
- **Defence underfunding**: Falling defence budgets hampered modernisation and equipment upgrades.
- **No clear security policy**: India lacked a comprehensive strategy to address evolving threats like proxy wars and regional nuclearisation.

Major initiatives taken for strengthening India's defence architecture in last fews decades

Specification	Reforms taken
Intelligence	• **National Technical Research Organisation (NTRO)** to protect **national critical infrastructure** and handling cyber-related issues. • **A Multi Agency Centre (MAC)** has been established for daily intelligence sharing.
National security management and apex decision-making	• **National Security Council (NSC)** was reformed to adopt whole of government approach. • **The Nuclear Command Authority,** set up in 2003, **has a** Political Council led by the Prime Minister that alone can authorize nuclear weapon use**.** • **Chief of Defence Staff (CDS)** created in 2019 is **the Permanent Chairman of the Chiefs of Staff Committee.**
Defence Modernisation	• **Agnipath Scheme** to ensure a balance between youthful and experienced personnel in the Armed Force. • **Defence production and indigenization:** DAP 2020, Positive Indigenisation List, SRIJAN Portal, ADITI (iDEX)

	• **Defence Offset Policy**: To **leverage capital acquisitions** to develop Indian defence industry
Border Management	• **Smart fencing: BOLD-QIT** (Border Electronically Dominated QRT Interception Technique) under **CIBM scheme.** • **Border Infrastructure and Management (BIM) Scheme** for the construction of border fence, border flood lights • **Vibrant Village Programme (VVP)**

Way ahead

Implementation of Recommendation of K. Subrahmanyam such as:

- Create an **organization** focused on **electronic and communication intelligence** (like the National Security Agency in US)
- **Publish war histories** and declassify official documents to establish the fact
- Create **synergy between military and the media**
- **Create civil-military liaison mechanisms at various levels**, from Command HQ to operational formations on ground to smoothen relationships.

Conclusion

Since the Kargil War, warfare has changed due to increased use of terror and irregular tactics by non-state actors, as well as advances in cyber and space technology. The Indian armed forces must be ready for future conflicts that may be more violent and unpredictable.

3.2. MARITIME SECURITY

3.2.1. MARITIME SECURITY AT A GLANCE

Maritime Security

Maritime Security involves **protecting the nation's sovereignty from threats arising from the oceans and seas**.

India's Security Architecture Post '26/11'

Indian Navy (IN) Responsible for overall maritime security.	**Indian Coast Guard (ICG)** Responsible for coastal security in the territorial waters, including areas to be patrolled by the marine police.	**Border Security Force (BSF)** Responsible for the security and surveillance of the **creeks in Gujarat and the Sunderbans.**	**Central Industrial Security Force (CISF)** Responsible for the **physical security of India's major ports**	**Sagar Suraksha Dal:** Fishermen groups, composed of trained volunteers, monitor the seas and coastal waters

Need of Maritime Security for India

Vulnerabilities of coastline Maritime terrorism **like 26/11 Mumbai attack**, Piracy, Smuggling, Infiltration through creeks.	**Geostrategic interests** Like countering Chinese influence, becoming a **net security provider** and executing **HADR operations in IOR.**	**Economic development** Around **80%** of India's **external trade and 90% of energy trade** happens through IOR.

Challenges to Maritime Security

Piracy and Maritime Terrorism in IOR E.g. Indian Navy rescued the hijacked **Bulgarian vessel 'Ruen'** in **2024.**	**Maritime Border Disputes** with neighbouring countries, **such as Pakistan, Sri Lanka**	**Rising Influence of USA and China** like Chinese dual-use facilities in **Myanmar and Sri Lanka**	**Lackadaisical State Government:** Issues include underused patrol boats, **delayed infrastructure**, manpower shortages, and unspent funds **(CAG Report).**	**Environmental Challenges: Climate change** (rising seas, extreme weather), **natural disasters** (tsunamis, cyclones) **Marine pollution** (Oil spills)

Steps taken by India to strengthen Maritime Security

Coastal Surveillance & Coordination Sagar Kavach coastal security exercises	**Maritime Theatre Command (MTC)** Proposed to create efficient deployment of maritime assets.	**Information Sharing IFC-IOR (Information Fusion Centre – Indian Ocean Region)** of Indian Navy	**Regional Maritime Cooperation Initiatives like SAGAR, MAHASAGAR, IORA,** and **IONS (Indian Ocean Naval Symposium)**	**Coastal Shipping Bill, 2024**

Way Forward to strengthen maritime security

5-point frame work Free trade, dispute resolution, connectivity, threat response, environmental protection	**Strengthening the surveillance system** Through advanced coastal radar networks. **E.g. High Frequency Radar**	**Unified Command Structure** Expedite the formation of a unified **Maritime Theatre Command** to ensure integrated operations.	**Operationalize Blue Economy Potential** Secure India's interests in **deep-sea mining, offshore energy**, and **sustainable fisheries**	**Boost Maritime Diplomacy** Deepen cooperation through **IORA, IONS, QUAD**, and **SAGAR** and conduct joint naval exercises to increase **interoperability** and trust

3.3. KEYWORDS

Keywords				
Infiltration	Cross-border terrorism	Insurgency	Geostrategic interests	Comprehensive Integrated Border Management System
BOLD-QIT	Border Protection Grid (BPG)	Line of Control (LoC)	Operation Vijay	Security Policy
Indigenization	Civil-military liaison	Maritime terrorism	Security Architecture	Net security provider
Maritime Theatre Command	Coastal Surveillance & Coordination	HADR operations	Blue Economy	

3.4. PRACTICE QUESTION

Answer Canvas

Discuss the strategic significance of maritime security for India and evaluate the steps taken to strengthen it after the 26/11 attack. Also, suggest a way forward to address existing challenges.

Introduction	Body Part: 1	Body part: 2	Conclusion
Define what is maritime security	Significance of maritime security	Measures & Challenges	Conclude by highlighting the need for joint command, regional cooperation, technological upgrades, and proactive maritime diplomacy.

4. SECURITY FORCES

4.1. DEFENCE MODERNISATION

4.1.1. MODERNISATION OF ARMED FORCES AT A GLANCE

Modernisation of Armed Force

Modernisation involves continuously **upgrading weapons, platforms, and technologies** to keep the armed forces ready for evolving security threats and strengthen overall defence capabilities.

Need for Modernisation of Armed Forces

Challenging strategic environment like assertiveness of China in Indian Ocean.	**Inadequate number of equipments** like aircraft, submarines etc.	**Rapidly changing landscape of warfare** like **hybrid warfare, cyberwarfare, etc.**	**Enhancing HADR capabilities** in which defence forces play the critical role.

Challenges in modernisation of Armed Forces

Budget Allocation Issues A large portion of the defence budget goes to salaries, pensions, Leaving **limited funds for capital expenditure** and R&D for new technology	**Slow Decision-Making**. It can take **7–9 years** to finalise production and acquisition contracts.	**Technological Limitations** India lacks the deep ecosystem to **indigenously design and manufacture** advanced defence systems and critical components.	**Stalled Structural Reforms** Important reforms like **Integrated Theatre Commands** are **delayed due to inter-service rivalries** and lack of consensus among the three forces.

Steps taken by India for mordernisation of Armed Forces

Defence Reforms 2025 declared as the **Year of Reforms, Inter-Services Organisations Act, 2023 and empowering Chief of Defence Staff (CDS)** to issue **joint orders** across all three forces to boosts coordination among 3 forces.	**Indigenisation and Innovation** Defence Acquisition Procedure (DAP) 2020, Positive Indigenisation List, and SRIJAN Portal, Schemes like **ADITI** and **iDEX** promote startups and MSMEs in defence.	**R&D Push** 25% of defence R&D budget reserved to promote **indigenous defence technology,** 74% FDI allowed via automatic route and 100% via government approval to boost investment.	**Space Warfare Preparedness Mission DefSpace** supports innovation in space-based defence applications; **Mission Shakti (ASAT)** to defend India's space assets from threats.

Way forward for mordernisation of Armed Forces

Ensure Steady Funding: Create a **Non-Lapsable Defence Modernisation Fund** (as proposed by the 15th Finance Commission).	**Implement Reforms** Set up **BRADS** (Board of Research for Advanced Defence Sciences) as recommended by the **Rama Rao Committee**.; **Shekatkar Committee** recommendations to boost combat capability and rebalance defence spending	**Boost Private Sector Role** Support industry using the **5Is** (Identify, Incubate, Innovate, Integrate, and Indigenous. Partnerships), **implementation strategy for AMCA project is** a positive step in this direction.	**Strengthen Collaboration** Build strong industry-defence-academia partnership

4.1.2. DEFENCE EXPORTS AT A GLANCE

India's Defence Export

Status of India's Defence Export

India's defence exports have **surged** to a record high of **₹23,622 crore** in the Financial Year (FY) 2024-25.	**Major Export Destinations:** India is among the **top 25 arms exporters**, supplying defence equipment to over 100 countries. Major buyers include the USA, France, and Armenia.	**Export Portfolio:** Includes Akash missiles, ATAGS artillery, naval vessels, and aircraft like LCA Tejas and ALH Dhruv.

Steps taken up to boost Defence exports

iDEX(Innovations for Defence Excellence) To support **startups, MSMEs, academia**, and R&D institutes for developing defence technologies.	**Defence Export Promotion Scheme (DEPC)** Launched to help **Indian manufacturers** promote their defence products globally and boost exports.	**Defence Industrial Corridors (DICs)** Set up in **Uttar Pradesh and Tamil Nadu** to promote indigenous defence manufacturing.	**Ease of Doing Busines** Simplified industrial licensing, Digitised export authorisation system etc.	**Liberalised FDI Policy (2020)** Allows up to **74% FDI via automatic route**, beyond that with government approval.

Key Challenges in Defence export

Import Dependence Key components like **engines, sensors**, and avionics still sourced from abroad.	**R&D Gap** Limited progress in **AI systems, stealth tech**, and hypersonic weapons.	**Global Competition** Faces stiff rivalry from established exporters like **USA, Russia, and France.**	**Regulatory Delays** Bureaucratic inefficiencies **in procurement** and approvals slow down progress.	**IPR Issues** India co-produces platforms like the T-90 tank and Su-30 jet with Russia, but the **IPR remains** with foreign OEMs.

Way Forward to enhance defence export

Export Complete Systems Target **regions like Africa, Southeast Asia, and Latin** America; use **EXIM Bank lines of credit to boost sales.**	**Focus on Subsystems** Encourage small manufacturers **to join global supply chains** by improving their component production capabilities.	**Promote Indian Defence Brands** Use international expos and trade fairs to showcase indigenous products and **leverage Defence Attachés** to identify export opportunities and promote Indian products abroad.	**Forge Global Partnerships** Collaborate with emerging defence hubs like Australia, UAE, Saudi Arabia, and South Korea **for joint manufacturing**, use **offset obligations** to encourage **foreign companies to source from Indian firms.**

4.1.3. INTEGRATED THEATRE COMMANDS (ITCS)

Why in the News?

The Defence Minister has empowered the **Chief of Defence Staff (CDS)** to issue **joint orders** for the Army, Navy, and Air Force, a **crucial step for creating ITC.**

More on the News

- The current direction replaces the old system, where each service issued separate orders, marking a **new step toward jointness and integration** in the Armed Forces.

- They are among the **nine priority areas** for defence reforms in **2025 (**declared as the "year of reforms"**).**
- **Jointness & Integration are pre-requisites** for the creation of functional **Integrated Theatre Commands (ITCs)**.

About ITCs

- **ITCs** involves **creating unified tri-service organisations** that would be **responsible for combat operations** (as well as internal security duties) in **specified geographic area**.
- The **single theatre commander will also control necessary assets** from all three services for combat or internal security tasks.
- Creation of such commands will **separate the 'operational' functions from the Raise-Train-Sustain (RTS)** and other administrative functions.
- They can **streamline procedures**, **cut redundancies**, and **boost coordination** among the services.
- The **Kargil Review Committee** in 2001 has recommended creation of ITCs.

Current Structure of Armed Forces

- There are 19 existing commands –
  - **17 single-service oriented commands** (7 Army, 7 Air Force, and 3 Navy).
  - **Andaman and Nicobar Command** and the **Strategic Forces Command** (in charge of the country's nuclear stockpile) function as tri-services commands.

Key Initiatives Supporting ITC

- **Inter-Services Organisation (Command, Control, and Discipline) Rules, 2025**: Enables unified control and discipline across services.
- **Chief of Defence Staff (CDS)**: Promotes joint operations, training, and logistics.
- **Department of Military Affairs (DMA)**: Established under Defence Ministry with CDS as Secretary.
- **HQ Integrated Defence Staff (IDS)**: Provides tri-service advice to the government.

Challenges in Creating ITCs

- No clear **National Security Strategy**.
- **Interoperability issues**: Different equipment and platforms across services.
- **Resource limitations**, especially for Air Force support across multiple theatres.

Conclusion

Integrated Theatre Commands aim to streamline India's military structure, increase jointness, and ensure faster, coordinated responses in modern warfare. While the intent is strong, addressing strategy, logistics, and interoperability remains crucial for successful implementation.

4.1.4. INDIAN COAST GUARD

Why in the News?

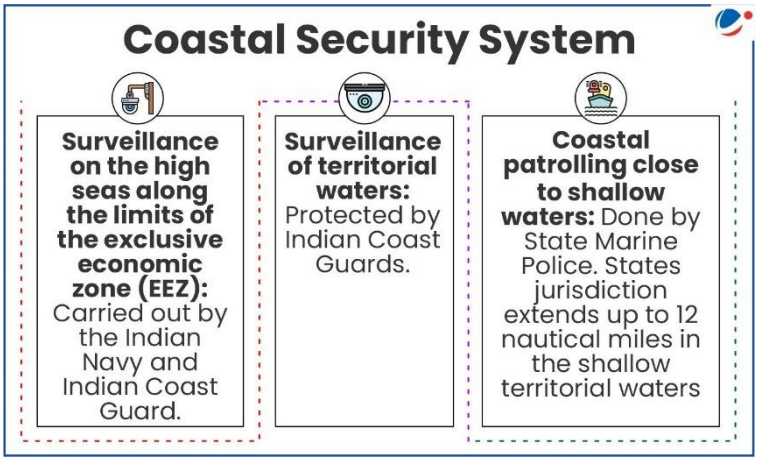
Parliamentary Standing Committee on Defence reviewed the **role of the Indian Coast Guard (ICG)** in ensuring coastal security.

About the Indian Coast Guard

- **Genesis:** Constituted under the **Coast Guard Act 1978**
- Nodal ministry: Ministry of Defence
- **Key role: ICG** plays a vital role in India's multi-layered maritime security setup (**refer to the infographic**). Some of its major functions include:
  - **National Coordinating Agency** for: Maritime Law Enforcement**;** Maritime Search & Rescue**, and** Marine Pollution Response
  - **Offshore Protection**: Patrols Offshore Development Areas (ODAs) on both coasts.

- **Anti-Smuggling**: Assists customs and agencies in blocking illegal goods.

Initiatives taken to strengthen Indian Coast Guard



- **Inter-agency Maritime Exercise:** ICG participates and conducts various maritime exercises and operations. E.g. **SAREX-2024, Sagar Kavach.**
- **Increased responsibility:** ICG was additionally designated as the authority responsible **for coastal security in territorial waters**, including areas to be patrolled by the Coastal Police.
- **Coordination between Central and State agencies:** The Director General of ICG, as Commander Coastal Command, **coordinates coastal security** between Central and State agencies.

Conclusion

Over the years, ICG has become a key maritime agency, strengthening India's search and rescue system. Through strong collaboration, it supports India's SAGAR vision, enhancing the country's role as a reliable maritime partner.

4.1.5. NATIONAL INVESTIGATION AGENCY (NIA)

Why in the news?

The Supreme Court in **Ankush Vipan Kapoor vs. NIA (2024)** ruled that the **NIA can investigate non-scheduled offences** if they are connected to scheduled offences under the NIA Act.

About the Case

- The case involved **drug trafficking**, **hawala channels**, and **terror funding**.
- Though **Narcotic Drugs and Psychotropic Substances (NDPS) Act, 1985 offences** are not scheduled under the NIA Act, the **Court allowed NIA to probe** them as they were **linked to scheduled crimes.**
  - **The court ruling was based on** broad interpretation of **Section 8 of the NIA Act**,

About National Investigation Agency (NIA)

- **Genesis:** Formed under the NIA Act, 2008 after the 26/11 Mumbai attacks to handle terrorism-related cases.
- **Objective**: Investigates and prosecutes offences that threaten India's **sovereignty, security, integrity, foreign relations, and international obligations**.
- **Scheduled Offences**: Covers laws like the Explosive Substances Act (1908), Atomic Energy Act (1962), UAPA (1967), and Anti-Hijacking Act (2016) etc.
- **Jurisdiction:** covers entire country, Indian citizens abroad, government officials anywhere in the world, individuals on Indian-registered ships and aircraft
- **Powers of NIA:**
  - **Investigation:** Central Government can direct NIA to investigate when it is of the opinion that a Scheduled Offence has been committed.
  - **Prosecution:** The NIA can prosecute cases in specially designated NIA courts.
  - **Coordination with State Police:** It collaborates with state law enforcement agencies during investigations.
  - **Extraterritorial Operations:** The agency can investigate and prosecute offences committed outside India, subject to international cooperation agreements.

- **Conviction rate:** Since its inception, the NIA has registered 640 cases, with judgments in 147 and a conviction rate of 95.23%.

Key initiatives to enhance the capacity of NIA

- **Increased Budget:** NIA's budget grew from **₹91.32 crore (2014-15)** to **₹394.66 crore (2024-25)**, showing the government's commitment to national security.
- **Technology & Data Analytics: National Terror Data Fusion & Analysis Centre (NTDFAC)** was set up to enable **Big Data Analytics**, automation, and digitization
- **Expanded Mandate:** The **NIA Amendment Act, 2019** broadened NIA's jurisdiction to include **Cyberterrorism, Human trafficking.**
- **Nodal Agency:** NIA is the Central Nodal Agency for investigating **Terror Funding, and Fake Indian Currency Notes (FICN)**
- **International Coordination:** A **Joint Task Force (JTF)** with **Bangladesh** supports real-time information exchange on FICN and cross-border crimes.

Conclusion

As the NIA evolves, its capacity to adapt to new challenges and coordinate with state and foreign organizations will be critical to effectively countering organized crime and terrorism.

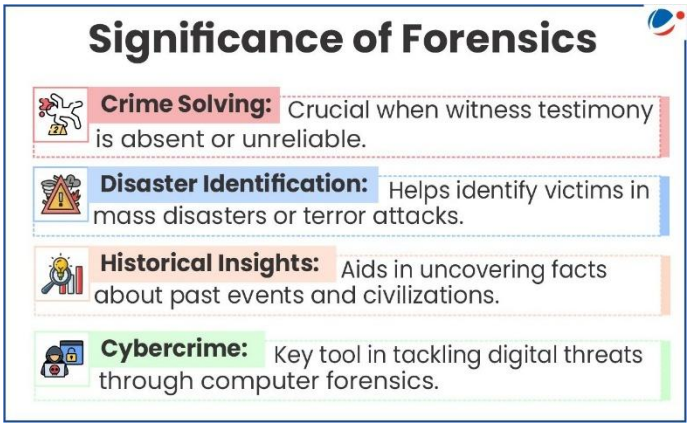
4.1.6. FORENSICS IN INDIA

Why in the News?

The Union Cabinet has approved **the National Forensic Infrastructure Enhancement Scheme (NFIES)** for 2024-25 to 2028-29.

About the Scheme

- **Nodal Ministry:** Ministry of Home Affairs
- **Purpose:** To meet the growing demand for forensic investigations under the **Bharatiya Sakshya Adhiniyam, 2023**, which **requires forensic probes** in crimes with punishment of **7 years or more**.
- **Key Components of NFIES**
  - **New Campuses** of the **National Forensic Sciences University (NFSU)**
  - **New Central Forensic Science Laboratories**
  - **Upgradation** of infrastructure at **NFSU-Delhi**



About Forensics:

- **Definition:** Application of scientific methods to investigate crimes and produce evidence for legal proceedings.
- **Key Techniques**: DNA profiling, fingerprint analysis, ballistics, toxicology, and digital forensics.

Challenges of Forensics in India

- **Funding Issues**: Low budget limits modernisation of labs and police facilities
- **Infrastructure Gaps**: Few and overburdened forensic labs, **40% staff shortage** (BPRD data), Outdated equipment, causing delays
- **Lack of Standard Procedures:** Absence **of uniform procedures** leads to inconsistent results, Evidence often rejected in court due to mishandling.
- **Institutional Problems**: Bureaucratic delays, weak coordination between police, labs & prosecutors

Way Forward

- **Implement Malimath Committee (2003) Suggestions**
  - **Coordination Bodies** at state/district level for better teamwork
  - **Year-long training** for new prosecutors & judges (with lab/court visits)
  - **Forensics in Education** (set up departments in universities, introduce basics in schools)
- **Other Key Measures**
  - **Cyber Forensics**: Expand I4C, train experts, open more cyber labs
  - **Public-Private Partnerships**: Involve private labs to clear backlog
  - **Global Cooperation**: Collaborate internationally for training & tech upgrades

Conclusion

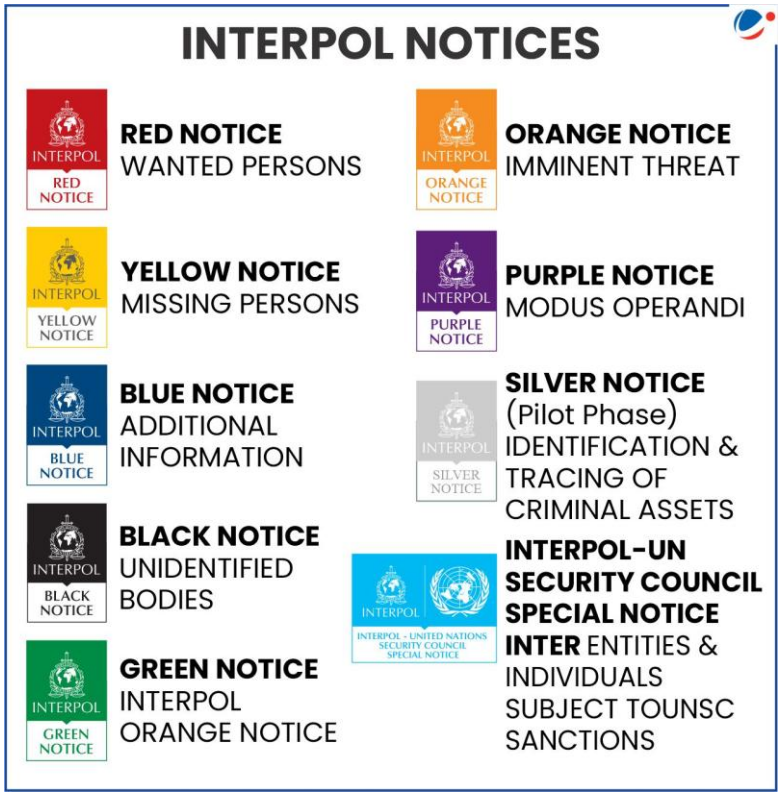
The National Forensic Infrastructure Enhancement Scheme is a timely move to boost India's forensic capacity and support faster, more effective criminal justice delivery under new legal rules

4.2. GLOBAL AGENCIES

4.2.1. INTERPOL

Why in the News?

The **INTERPOL** has issued the **silver notice on India's request to track the global assets of former French Embassy officer** Shubham Shokeen, who is **wanted in connection with a visa fraud.**



About Silver notice

- Silver Notice is the **newest addition to the INTERPOL's colour-coded Notices.**
  - INTERPOL's **colour-coded notices** are **international requests for cooperation or alerts** allowing police in member countries to share critical crime-related information **(refer to the infographic)**
- **Purpose**: Allows tracing and gathering information on assets of fugitives and key accused, even if the assets are in foreign countries.
- **Global Collaboration**: India is one of 51 countries participating in the first phase of this Interpol pilot project, running at least until **November 2025**.
- **First Use**: The **first Silver Notice** was issued in **January** on behalf of **Italy**.
- **Limit**: Each country can request up to **9 Silver Notices** during the pilot phase.

About INTERPOL

- **Headquarters:** Lyon, France.
- **Genesis:** Established as **International Criminal Police Commission (ICPC)** during 2nd International Police Congress in Vienna in **1923** and **stablished as INTERPOL in 1956**
- **Members:** 196 countries (India a founding members).

- **National Central Bureau (NCBs):** Established by member countries as a **point of access for INTERPOL affairs.**
  - **CBI is India's NCB** to the INTERPOL and it has also developed **Bharatpol portal for better coordination**
- **Governing Bodies:** The General Assembly and Executive Committee.

Need for International Police Cooperation

- **Cross-border crimes:** Crimes such as money laundering, trafficking, and smuggling operate across international borders.
  - For example, **INTERPOL's Operation HAECHI** improved global cooperation against cyber financial crimes.
- **Modern threats**: Cybercrime, radicalization, and trafficking exploit legal gaps. **Example**: INTERPOL's **Operation Serengeti** arrested over 1,000 cybercriminals affecting 35,000 victims across 19 African countries.
- **Counter-terrorism**: Sharing intelligence and coordinated actions are vital to disrupt **terrorist networks** involved in funding, recruitment, and attacks worldwide.
- **Legal support**: **Operation FLASH-WEKA**, with 54 countries, dismantled human trafficking networks in Africa.
- **Resource sharing**: Pooling resources boosts **intelligence sharing**, **crime control**, and response to emerging threats.

Obstacles in International Police Cooperation

- **Legal and Procedural Disparities:** Differences in laws and standards cause conflicts in investigations and prosecutions.
- **Cultural Barriers:** Language gaps, cultural clashes, and corruption hinder trust and communication.
- **Resource Constraint:** Disparities in technological capabilities hinder seamless information sharing and restrict participation in joint operations.
- **Political indifference:** Political tensions and conflicting national interests hinder comprehensive cooperation.

Conclusion

While challenges like jurisdictional conflicts, legal differences, and data privacy concerns persist, continuous collaboration, technological advancements, and diplomatic efforts can strengthen global policing efforts. As crime continues to evolve in an increasingly interconnected world, international police cooperation remains indispensable in fostering a safer and more just global society.

4.3. KEYWORDS

Keywords					
Warfare Preparedness	Mission Shakti (ASAT	Hybrid warfare	Cyberwarfare	Cyber Forensics	Integrated Theatre Commands
Non-Lapsable Fund	National Coordinating Agency	Industry-defence-academia partnership	Hawala channels	Defence Industrial Corridors	Offshore Protection
Offshore Development Areas (ODAs)	Fake Indian Currency Notes (FICN)	Extraterritorial Operations	Data Analytics	Joint Task Force (JTF)	Cultural Barriers
Jurisdictional conflicts	Public-Private Partnerships	BRADS (Board of Research for Advanced Defence Sciences	Ease of Doing Business	Colour-coded Notices	National Central Bureau (NCBs)

4.4. PRACTICE QUESTION

Answer Canvas

India's reputation as a trusted partner in defence exports is built on its commitment to quality, reliability, and meeting the specific needs of its partners. Critically evaluate this statement.

Introduction	Body Part: 1	Body part: 2	Conclusion
Mention the current status of defece export (monetary value, major export destinations and major export portfolio)	Mention initiatives that underscore India's defence products' quality, reliability, etc.	Throw some light on the key challenges faced by India's defence export	Conclude by highlighting the reform that needs to be taken to further strengthen the defence export.

5. MISCELLANEOUS

5.1. RISE IN NUCLEAR WEAPONS ARSENAL

Why in the News?

The Stockholm International Peace Research Institute (SIPRI) released its **SIPRI Yearbook 2024** highlighting a **concerning rise in nuclear weapon development** and **deployment.**

Key Findings

- **Global Nuclear Stockpile Decline:** Since the end of the Cold War, the number of **retired warheads has exceeded new deployments.**
- **Countries Expanding Stockpile: China** is expanding fastest, with its stockpile now at least **600 warheads**.
  - **India's arsenal** increased from **172 to 180** warheads, more than Pakistan's (170).
- **Modernisation:** In **2024**, all **9 nuclear-armed countries** continued to **modernise their arsenals**.
- **Status of Fissile Materials:** The explosive material utilized in nuclear weapons is fissile material, either **highly enriched uranium (HEU) or separated plutonium**.
  - **China, and Pakistan** have produced **both HEU and plutonium** for use in their nuclear weapons.
  - **India and Israel** have produced **mainly plutonium.**
- **Emerging Threats:**
  - **Modern Technologies:** The rapid development of **artificial intelligence (AI), cyber capabilities, space assets, missile defence and quantum** are radically creating potential sources of instability.
  - **Arms control in crisis:** While **New START** remains **in force until early 2026,** there are no signs of negotiations to renew or replace it.

Why Nations Pursue Nuclear Weapons?

Security Deterrence	Domestic Political Pressures	Prestige & Norms
Balance of Terror**": Nations like India acquire** nukes to counter nuclear-armed rivals (**e.g.,** China-Pakistan axis).	"**Nuclear Lobbies":** Military, scientists, and politicians push for arsenals to boost institutional power.	**Great Power Symbol:** Nuclear status grants geopolitical influence (e.g., UNSC permanent seats correlate with nuclear capability).

Threats Posed by Nuclear weapons

- **Rising Nuclear Risks**: **Geopolitical tensions** delay disarmament (e.g., Russia exiting New START, CTBT delays). **Nuclear threats** from Russia and North Korea increase fears of escalation.
- **Risk of Nuclear Accidents**: Attack on **Zaporizhzhia plant** (Ukraine, 2024) raised global radiation concerns.
- **Emerging Challenges**: **Cyber threats**: Risk of hacking nuclear command systems.
- **Space-based nukes**: Can cause EMPs, destroy satellites, and create debris.
- **Threats Specific to India:**
  - **China's Nuclear Expansion:** Possible shift from **No First Use** and limited deterrence raises regional concerns.
  - **Pakistan's Nuclear Posture: Tactical Nuclear Weapons (TNWs) d**esigned to counter India's **Cold Start Doctrine,** Lower nuclear threshold due to **no "No First Use" policy**.

Major initiatives to Prevent Nuclear Proliferation

- **International Atomic Energy Agency (IAEA):** Established in 1957 as an autonomous international organisation within the UN for promoting the safe, secure and peaceful use of nuclear technology.
- **Nuclear Weapons (NPT), 1970: A binding international treaty whose objective is to prevent the spread of nuclear weapons and weapons technology. India, Israel, and Pakistan** have never joined, while **North Korea withdrew in 2003.**

- **Partial Test Ban Treaty 1963:** Treaty banning nuclear weapon tests in the atmosphere, in outer space and underwater (India has signed and ratified).
- **Comprehensive Nuclear Test Ban Treaty (CTBT), 1996:** CTBT bans all nuclear explosions, whether for military or peaceful purposes (India did not sign)
- **Prohibition of Nuclear Weapons (TPNW) 2017**: includes a comprehensive set of prohibitions on participating in any nuclear weapon activities (India did not sign).
- **New START Treaty (2011):** Bilateral nuclear arms control treaty between Russia and the United States

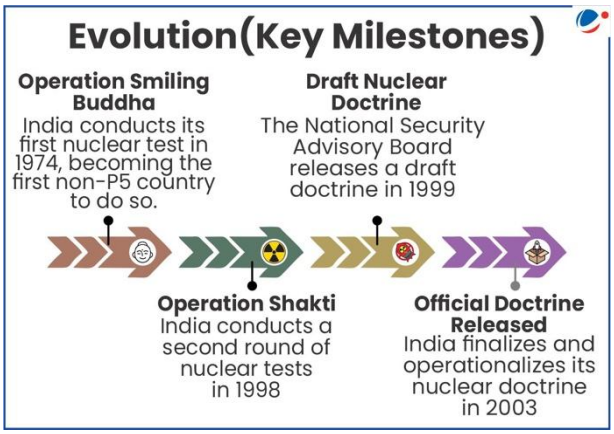
Conclusion

The global rise in nuclear arsenals poses a serious threat to peace, stability, and humanity. While nuclear weapons are often justified as deterrents, their very existence keeps the world on edge. The joint statement by the five nuclear-weapon states— "a nuclear war cannot be won and must never be fought"—must serve as a guiding principle.

5.2. 25 YEARS OF INDIA'S NUCLEAR DOCTRINE

Why in the news?

India is celebrating 25 years of its **nuclear doctrine launch.**



About India's Nuclear doctrine

- Nuclear Doctrine encompasses the **goals and missions that guide the deployment and use of nuclear weapons**.
- **Key Features**
  - **Credible Minimum Deterrence:** Maintain a limited but effective nuclear arsenal to deter adversaries.
  - **No First Use Policy**: Nuclear weapons will only be used in response to a nuclear attack on India or its forces.
  - **Massive Retaliation**: Any nuclear strike against India will face a large-scale and devastating response.
  - **No Use Against Non-Nuclear States**: Nuclear weapons will not be used against countries without nuclear arms.
  - **Support for Disarmament**: Committed to a nuclear-free world through global, verifiable, and fair disarmament efforts.
  - **Governance Structure**
    - **Political Council** (headed by PM): Final authority on nuclear strike decisions.
    - **Executive Council** (led by National Security Advisor): Advises and handles implementation.

Efficacy of No First Use

It remains the **most debated element of India's nuclear doctrine.**

Aspect	Against NFU	In Favour of NFU
Risk of Initial Casualties	May cause **high casualties** if India suffers the first strike.	Contributes to **India's strategic restraint posture** and **enables civil nuclear cooperation agreements** and accommodation in multilateral nuclear export control regimes.
Ballistic Missile Defence (BMD)	An **elaborate and costly BMD system required** to defend against a first strike.	NFU helps India maintain a **defensive and non-escalatory stance.**

Effectiveness Against Nuclear neighbours	Ineffective against Pakistan, which is lowering its threshold with **Tactical Nuclear Weapons** (low-yield weapons to be used in their own territory against Indian forces).	A **prudent and non-escalatory approach** to **managing tensions with China** and contributes to regional stability.

How can the present nuclear doctrine be strengthened?

- **Policy initiatives:** Launch targeted programs like the **Integrated Missile Development Programme** to boost capability alongside tech advancements.
- **Introduce Strategic Flexibility**: Incorporating **ambiguity** could allow proportionate retaliation, especially against tactical nuclear weapons, without triggering full-scale war.
- **Align with Foreign Policy**: Regularly **update the doctrine** in line with global shifts to reflect changing threats and alliances, including the **China-Pakistan-Russia nexus.**
- **Promote Non-Proliferation Leadership**: Engage in global platforms like the **Conference on Disarmament** to encourage broader **adoption of No First Use.**

Conclusion

India's nuclear doctrine balances **credible deterrence** with a commitment to restraint through its **No First Use policy and support for global disarmament**. While it maintains a strong defensive posture, evolving regional threats **call for strategic flexibility and technological upgrades.**

5.3. BIOLOGICAL WEAPONS CONVENTION (BWC)

Why in the News?

United Nations Office for Disarmament Affairs (UNODA) celebrated 50th anniversary Biological Weapons Convention (BWC) that entered into force in 1975.

About BWC

- It is **the first multilateral disarmament treaty** that **bans an entire class of Weapons of Mass Destruction (WMD).**
  - It prohibits the development, production, stockpiling, acquisition, transfer, and use of biological and toxin weapons.
- **Biological weapons**: They are tools of war designed to **spread harmful organisms**—such as bacteria, viruses, fungi, or toxins—to **cause disease or death** in humans, animals, or plants.
- **Membership:** 188 member states (including India)

Measures taken by India to implement Biological Weapons Convention (BWC)

- **1989 Rules on Hazardous Microorganisms**: Regulate the use, storage, import, export, and manufacture of genetically engineered organisms to protect health and the environment.
- **Weapons of Mass Destruction Act, 2005**: Bans unlawful activities related to weapons of mass destruction, including their delivery systems.
- **SCOMET (Special Chemicals, Organisms, Materials, Equipment and Technologies) List:** India's export control list includes microorganisms and toxins under Category 2 to **regulate dual-use biological items**.
- **India-France Proposal**: Both countries proposed a database to support assistance under **Article VII of the BWC**, which ensures help for any state affected by a BWC violation.

Key Challenges in BWC Implementation

- **No Verification Mechanism**: The **dual-use nature of bioscience** makes it hard to distinguish peaceful from offensive use, unlike other disarmament treaties.
- **Weak Data Collection**: The BWC lacks binding data reporting rules and depends on **voluntary confidence-building measures** (CBMs), which have low participation (just over 50% in 2022).

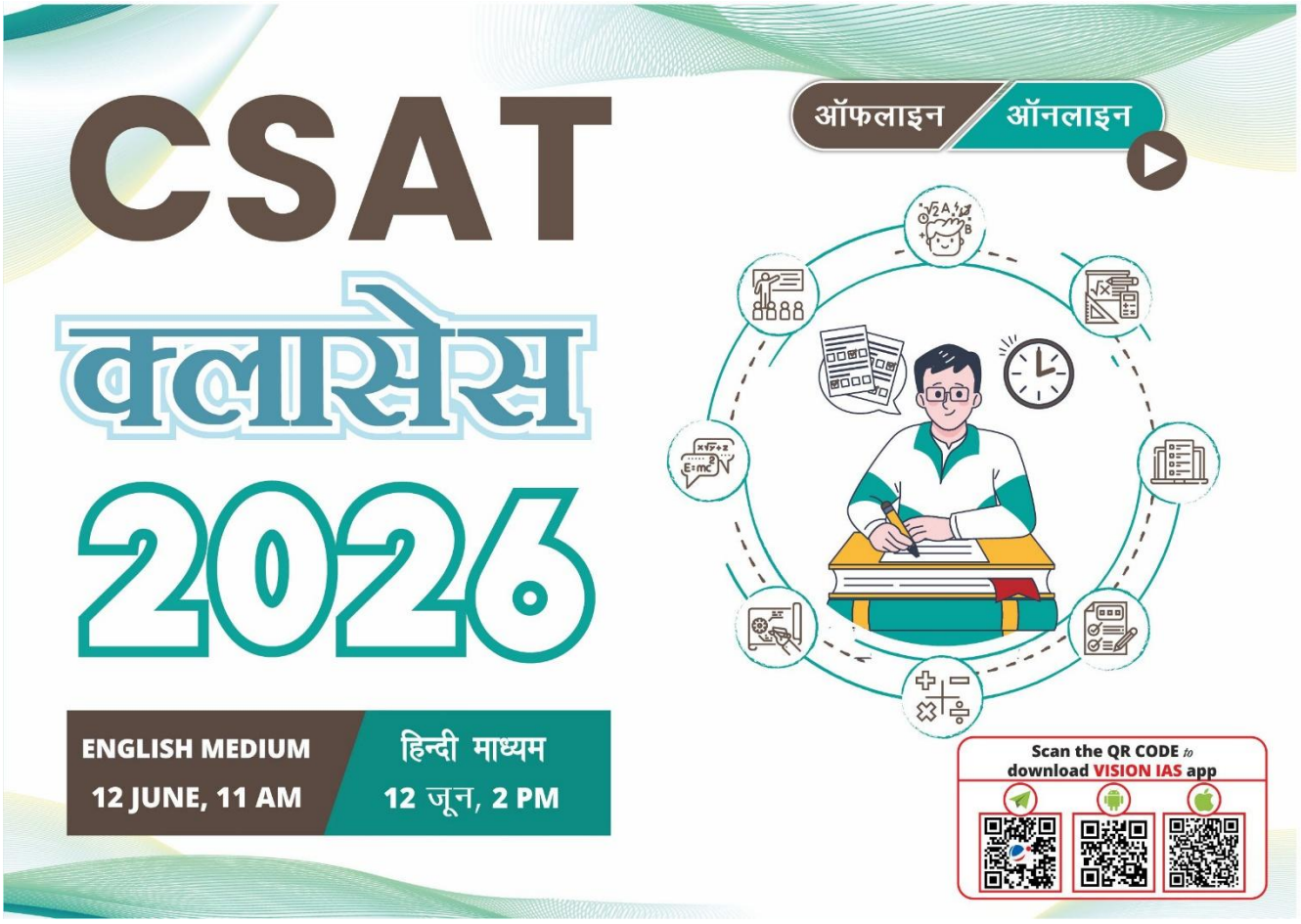
- **Limited Institutional Support:** The Implementation Support Unit remains **understaffed**.
- **Gaps in National Enforcement**: India, for instance, has **no central authority** for BWC, unlike for the Chemical Weapons Convention.

Way Forward to enhance the effectiveness of BWC

- **Strengthen Verification:** Use a modular, **step-by-step approach** combining policy tools and science for effective monitoring.
- **Enhance Institutional Capacity**: Create a **rotating expert group** under the United Nations Secretary-General to monitor compliance.
- **Improve CBMs**: Use **artificial intelligence tools like data harmonization** and text mining to simplify and encourage CBM reporting.
- **Counter Non-State Actor**: Align BWC with United **Nations Security Council Resolution 1540** to block terrorist access to biological weapons.

Conclusion:

The Biological Weapons Convention is vital for global disarmament, but challenges like weak verification, poor enforcement, and non-state threats remain. Stronger oversight, better institutions, and global cooperation are essential for its success.



5.4. DRONES FOR DEFENSE AT A GLANCE

Drones or Unmanned Aerial Vehicle (UAV)

- A UAV is an **unmanned aircraft system** that **is either controlled remotely or can fly autonomously without the need for a pilot.**
- **Drone technology for defence in India: Lakshya and Nishant**(DRDO's unmanned aerial systems),**Black Kite, Golden Hawk, Pushpak**(Micro and mini drones by DRDO), **Rudrastra a** Hybrid UAV with VTOL (**vertical takeoff and landing) c**apacity

Types of Drones

Based on Weight (as per Drone Rules, 2021)	Based on the Structure of the Lift Surface
Nano ≤250 g; **Micro** 250 g – 2 kg; **Small** 2 kg – 25 kg; **Medium** 25 kg – 150 kg; **Large-Greater than 150 kg**	**Rotary-wing Drones:** Rotor rotates to tilt by using articulating blades to push wind downward and vertically lift themselves. It could be **Single-rotor or Multi-rotor** **Fixed-Wing:** Rigid wings like aircraft, deal for long-range and heavy loads **Hybrid VTOL:** Mix of rotary and fixed-wing, and Vertical takeoff Horizontal flight

Significance of Drones for Defense

Intelligence & Surveillance (ISR)	Precision Attack	Tactical Edge
Monitor enemy movements, terrain, and installations.	Uses guided munitions to target enemies accurately, minimize collateral damage	Low-cost, low-risk solution with high efficiency. Boosts coordination, especially in border or mountainous zones.

Security Concerns with drones

Weaponized drones	Infrastructure disruption	Disruption to Air Defence System	Privacy threat
Drones could be modified for targeted attacks using explosives or weapons or **cross-border smuggling**	Cyber-attacks, jamming, physical damage.	**Drone swarms** can overwhelm radar and missile defences, making interception difficult. **Fibre optic drones** are **jam-proof**, with better **stealth and precision**, increasing the threat further.	Surveillance using HD cameras.

Initiatives taken to Tackle Drone Security Threats

Counter Drone System (D4)	Tech Review Panel	Border Deployment:	Border Deployment
Detects, tracks, and neutralizes drones in real time; **Bhargavastra is** India's first micro-missile to counter drone swarms.	MHA set up a committee to certify anti-drone technologies.	Anti-drone tech used, especially along the Punjab border.	**Anti-drone tech** used, especially along the Punjab border.

Way forward to counter security threats from drones

National Strategy	Secure Supply Chain	Private Sector Involvement
Develop a comprehensive plan to prevent misuse by terrorists and non-state actors.	Track UAV transfers, enforce codes of conduct, and ensure due diligence.	Partner with industry for early detection, tech innovation, and rapid response.

5.5. FIFTH-GENERATION FIGHTER JET AMCA

Why in the News

The Defence Minister has approved an **execution model** for India's indigenous **5th-generation fighter jet** named **Advanced Medium Combat Aircraft (AMCA).**

AMCA Programme Overview

- **Background:** Received approval from the Cabinet Committee on Security (CCS) in **2024.**
- **Purpose:** To manufacture the **indigenous 5th generation fighter jet aircraft** AMCA**.**
- **Timeline:** Prototype expected by 2028-29; induction targeted by 2034-35
- **Variants:** AMCA Mk1 with GE-F414 engines; Mk2 planned with indigenous engines.
- **Lead Agency:** Aeronautical Development Agency (ADA) under DRDO.
- **Industry tie-up:** Both **private and public sector companies** can bid independently, as joint ventures, or consortia on a **competitive basis**.
  - All entity/bidders must be **Indian companies** compliant with the national laws and regulations.

About the 5th Generation Fighter Jet

- The concept of fighter jet generations emerged in the 1990s and has been applied retrospectively to earlier jets.
  - **The first-Generation** fighter jets are Introduced in the late stages of **World War II**.
- However, there is **no strict definition** of each generation — the idea mainly helps understand broad technological leaps. A new generation begins when **a major innovation can't be added** to older jets through upgrades.
- The **5th Generation Fighter Jet are most advanced** in service today. They offer:
  - **Twin-engine powered:** Provides **higher level of air safety** in the event of failure of one engine especially at night.
  - **Stealth Capabilities**: They have **Low-Probability-of-Intercept Radar (LPIR)** and are harder to detect by enemy radar.
  - **Agile Airframes with Super cruise**: High manoeuvrability and the ability to fly at supersonic speeds.
  - **Advanced Avionics and Integrated Computer Systems**: Enables networking with other systems, giving pilots a 360-degree battlefield view without manoeuvring.
- **Examples:** Only the **US (F-22 and F-35), Russia (Sukhoi Su-57), and China (Chengdu J-20) have developed** operational fifth generation aircraft.

Strategic Importance of 5th Generation Fighter Jet AMCA

- **IAF Modernisation:** Fills critical capability gap post-MiG-29/Mirage phaseout, helps restore IAF's depleted squadron strength (31 vs. approved 42).
- **Regional Threat Dynamics:** Counters China's J-20 and Pakistan's J-10C (procured from China) deployments.
- **Technological Sovereignty:** Reduces dependency on foreign platforms, enhances long-term defence autonomy through Make in India.
- **Atmanirbhar Bharat:** The project will give a significant push towards enhancing India's indigenous defence capabilities and **fostering a robust domestic aerospace industrial ecosystem.**

Conclusion

To ensure the successful execution of the AMCA programme, a **multi-pronged strategy** is essential. The government must create an enabling ecosystem by easing **land acquisition norms**, investing in **defence-specific industrial infrastructure**, and supporting private sector capability by **leveraging HAL's experience.** A framework of investment and IPR laws to facilitate technology transfers specific to this programme is also essential.

5.6. INDIA'S AIR DEFENCE SYSTEM (ADS)

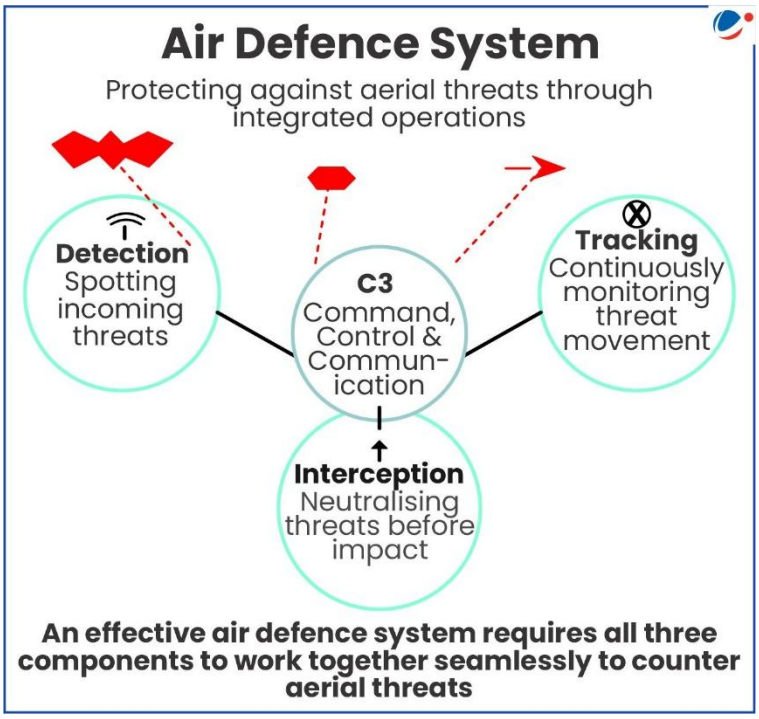
Why In the News?

India's Air Defence System (ADS) successfully thwarted attacks on India's Western Border during operation Sindoor.

About India's ADS

India's ADS consists of an **Integrated Counter UAS (Unmanned Aerial Systems) Grid**, where following **surface-to-air missile (SAM) systems** played a key role. Key Technologies of India's include:

- **S-400 Triumf (Acquired from Russia)**
  - Also called **Sudarshan Chakra** in India.
  - Among the **most advanced long-range SAMs in the world.**
  - Equipped with a **command-and-control system, phased array radars** and **electronic warfare countermeasures.**
  - Offers complete **360-degree radar and missile coverage.**
  - Multi-missile compatibility **enables layered defence.**
  - Can track and engage **multiple targets at once**
  - **Range & Capability**
    - **Tracking:** Up to 600 km
    - **Engagement: Up to 400 km**
    - **Altitude Coverage: From 30 meters to 30 km (**effective against low drones to high-altitude aircraft and missiles)



- **Barak 8 (Jointly developed by India and Israel)**
  - **Medium- to long-range (MR SAM or LR SAM)**
  - Equipped with **Mach 2 speed.**
  - Capable of **simultaneously engaging multiple targets** in the air.
  - **Range up to 100 km**
  - Both **maritime and land-based variants** of the system exist.
- **Akash Weapon System (Indigenously Built)**
  - **Short Range SAM**
  - Equiped with **built-in Electronic Counter-Counter Measures (ECCM)**.
  - Can simultaneously e**ngage Multiple Targets in Group Mode or Autonomous Mode.**
  - **Range & Capability**
    - **Range:** 4.5 km to 25 km
    - **Altitude of Operation:** 100 m up to 20 km
  - High **immunity against active and passive jamming.**
  - **Fully automatic** with quick response time from detection to kill.
  - **Guidance System:** Command Guidance

Conclusion

India's Air Defence System (ADS) plays a vital role in safeguarding the nation's airspace against evolving threats, including drones, missiles, and aerial intrusions. With growing technological challenges, it must continue to adapt through indigenous innovation, modernisation, and integration of layered defence.

5.7. MULTIPLE INDEPENDENTLY TARGETABLE RE-ENTRY VEHICLE (MIRV) TECHNOLOGY

Why in the News?

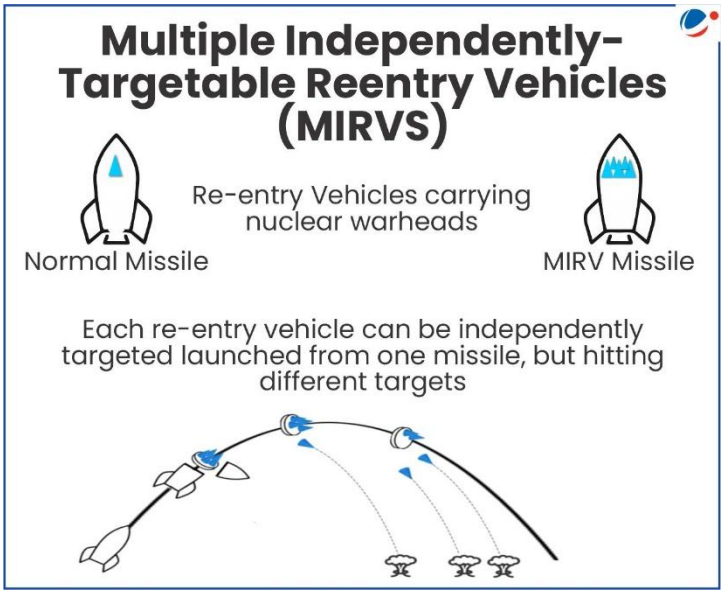
DRDO successfully tested the indigenous **Agni-5 missile** with **MIRV technology** under **Mission Divyastra**.

About MIRV technology

- **MIRV** allows one missile to carry **multiple nuclear warheads**, each aimed at a **different target**.
- **Warheads** are released at **different speeds and angles.**
- Can be launched from **land** or **submarine-based** platforms.
- Effective against **Ballistic Missile Defences (BMDs)** due to multiple, hard-to-intercept warheads.

Significance of Mission Divyastra and India's MIRV Capability

- **Stronger Deterrence:** Boosts **second-strike capability**, aligning with India's **No First Use and massive retaliation policy.**
- **Counter to Regional Threats**: China has MIRVs and Pakistan is developing MIRV (**Ababeel),** but India's use of Agni-5 gives it a clear edge in range and capability.
- **Technological Advancement**: Demonstrates India's ability in miniaturized warheads, precision guidance, and indigenous missile systems.
- **Global Recognition:** Places India among a **few nations with operational MIRV capability** (US, Russia, China, UK, France).



Challenges in MIRV technology

- **Vulnerability of Land-based MIRVs:** They put multiple warheads at risk if the missile is destroyed.
- **Arms Race Trigger:** MIRVs **can encourage first-strike strategies,** increasing arms race and instability.
- **Technical Hurdles:** Requires warhead miniaturization, **advanced guidance systems, and more fissile material like plutonium.**

Conclusion

India's successful Agni-5 MIRV test boosts its nuclear deterrence, counters regional threats, and highlights advanced missile tech. Despite this, challenges like vulnerability and arms race risks persist.

5.8. DIRECTED ENERGY WEAPONS

Why in the News?

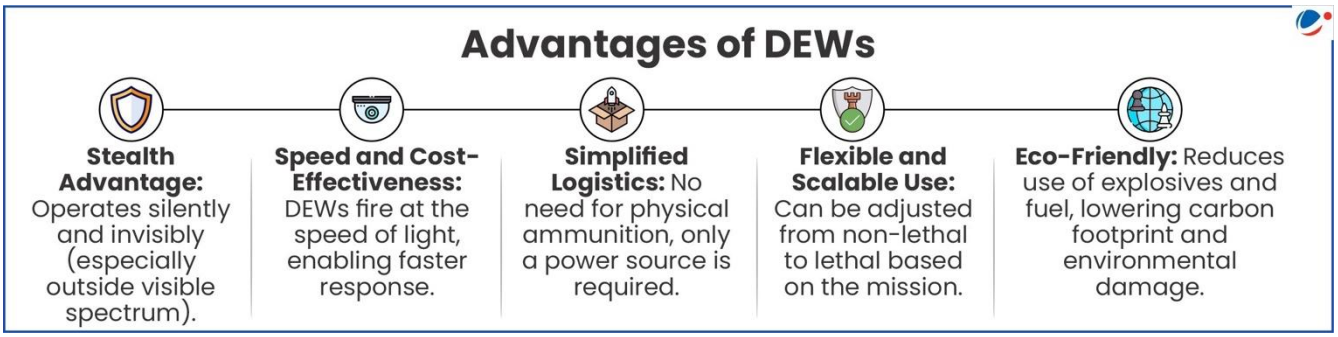
India has recently made major investments in **Directed Energy Weapons (DEWs)**.

What are Directed Energy Weapons (DEWs)?

- **DEWs** are ranged weapons that **use concentrated energy** from **electromagnetic** or **particle technology,** rather than **kinetic energy** to disable or destroy enemy equipment, facilities, and/or personnel.
- **Types of Directed Energy Weapons (DEWs)**
  - **High Energy Lasers (HEL):** Use focused light to **destroy targets.**
  - **High Power Microwaves (HPMs):** Emit electromagnetic waves **to damage electronics;** shorter range than HEL.

- **Millimeter Waves:** Used **for non-lethal** uses like crowd control; operate at short wavelengths (1–10 mm).
- **Particle Beam Weapons:** Use **fast-moving particles** (like protons or electrons) to cause damage.

- **Applications**
  - **Military:** Shoot down missiles, drones, and disable enemy electronics.
  - **Border & Law Enforcement:** Non-lethal use for crowd control.
  - **Space Operations:** Protect satellites from threats like space debris and enemy attacks.



Challenges of DEWs

- **Technological Limitations**:
  - Weather (fog, rain, dust) reduces laser effectiveness and range.
  - **Continuous monitoring** is needed to **maintain energy density and prevent degradation** due to debris or aging components.
- **Operational Risks:** Wide-beam DEWs (like High Power Microwave) can unintentionally affect friendly assets in the target area.
- **Health and Ethical Concerns**: Long-term effects on humans are still unclear, raising ethical and legal concerns over their use.

Steps taken by India for DEWs

- **Directionally Unrestricted Ray-Gun Array (DURGA)-II Project:** By DRDO to build 100-kilowatt lightweight DEW.
- **2kW DEW System:** Developed by BEL or countering new threats like drones.
- **Laser Science and Technology Centre (LASTEC) of DRDO:** Working for the development of laser source technologies for DEW.
- **Kilo Ampere Linear Injector (KALI):** A linear electron accelerator for targeting long-range missile

Conclusion

Given the persistent threat posed by its neighbours, particularly China and its vast technological prowess, India's defence needs to be prepared to deal with inevitable threat posed by both autonomous and hypersonic weapons, with DEWs as a potential solution.

5.9. KEYWORDS

Keywords				
Enriched uranium	Space assets	SIPRI	Nuclear Lobbies	Cyber capabilities
Credible Minimum Deterrence	No First Use	Tactical Nuclear Weapons (TNWs)	Nuclear States	Ballistic Missile Defence (BMD)
Tactical Edge	Integrated Missile Development Program	Weapons of Mass Destruction (WMD)	Massive Retaliation	Strategic Flexibility
Intelligence & Surveillance (ISR)	First-strike strategies	Air Defence System	Biological weapons	Advanced Guidance systems

5.10. PRACTICE QUESTION

Answer Canvas

India's nuclear doctrine reflects a balance between credible deterrence and strategic restraint. In the backdrop of changing regional and global security dynamics, critically assess the relevance and limitations of the doctrine after 25 years of its adoption.

Introduction	Body Part: 1	Body part: 2	Conclusion
Formally adopted in 1999 (articulated in 2003), India's nuclear doctrine aims at deterrence, responsible use, and global disarmament.	Key Features of the Doctrine	Evolving Challenges & Need for Reforms	Conclude by highlighting that doctrine remains a relevant moral and strategic framework but must adapt to evolving threats.

6. SECURITY PREVIOUS YEAR QUESTIONS 2013-2024 (SYLLABUS-WISE)

Linkages between development and spread of extremism, Role of external state & non-state actors in creating challenges to internal security

- Naxalism is a social, economic and developmental issue manifesting as a violent internal security threat. In this context, discuss the emerging issues gest a multilayered strategy to tackle the menace of Naxalism. (2022 15 marks)
- 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 15 Marks)
- The banning of 'Jammat-e-Islami' in Jammu and Kashmir brought into focus the role of over-ground workers (OGWs) in assisting terrorist organizations. Examine the role played by OGWs in assisting terrorist organizations in insurgency affected areas. Discuss measures to neutralize influence of OGWs. (2019 10 Marks)
- Indian Government has recently strengthened the anti-terrorism laws by amending the unlawful Activities (Prevention) Act (UAPA), 1967 and the NIA act. Analyze the changes in the context of prevailing security environment while discussing the scope and reasons for opposing the UAPA by human rights organizations. (2019 15 Marks)
- What are the determinants of left-wing extremism in Eastern part of India? What strategy should Government of India, civil administration and security forces adopt to counter the threat in the affected areas? (2018 15 Marks)
- 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 10 Marks)
- The North-Eastern region of India has been infested with insurgency for a very long time. Analyze the major reasons for the survival of armed insurgency in this region. (2017 10 Marks)
- 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 12.5 Marks)
- Article 244 of the Indian Constitution relates to administration of scheduled areas and tribal areas. Analyse impact of non-implementation of the provisions of the Fifth schedule on the growth of Left Wing extremism. (2013 10 Marks)

Challenges to internal security through communication networks, Role of media and social networking sites in internal security challenges, Basics of cyber security

- Explain how narco-terrorism has emerged as a serious threat across the country. Suggest suitable measures to counter narco-terrorism (2024 10 Marks).
- What are the different elements of cyber security ? Keeping in view the challenges in cybersecurity, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy (2022 15 marks).
- Keeping in view India's internal security, analyse the importance of cross-border cyber attacks. Also discuss defensive measures against these sophisticated attacks. (2021 10 Marks)
- Discuss different types of cybercrimes and measures required to be taken to fight the menace. (2020 10 Marks)
- What is CyberDome Project? Explain how it can be useful in controlling internet crimes in India. (2019 10 Marks)
- Data security has assumed significant importance in the digitized world due to rising cybercrimes. 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 protection of personal data in cyber space? (2018 15 Marks)

- Discuss the potential threats of Cyber-attack and the security framework to prevent it. (2017 10 Marks)
- Mob violence is emerging as a serious law and order problem in India. By giving suitable examples, analyse causes and consequences of such violence. (2017 15 Marks)
- Use of 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 12.5 Marks)
- Discuss the advantages and security implications of cloud hosting of servers vis-a-vis in-house machine-based hosting for government businesses. (2015 12.5 Marks)
- Religious indoctrination via digital media has resulted in Indian youth joining the ISIS. What is ISIS and its mission? How can ISIS be dangerous to the internal security of our country? (2015 12.5 Marks)
- 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 12.5 Marks)
- What are social networking sites and what security implications do these sites present? (2013 10 Marks) Cyber warfare is considered by some defense analysts to be a larger threat than even Al Qaeda or terrorism. What do you understand by Cyber warfare? Outline the cyber threats which India is vulnerable to and bring out the state of the country's preparedness to deal with the same. (2013 10 Marks)

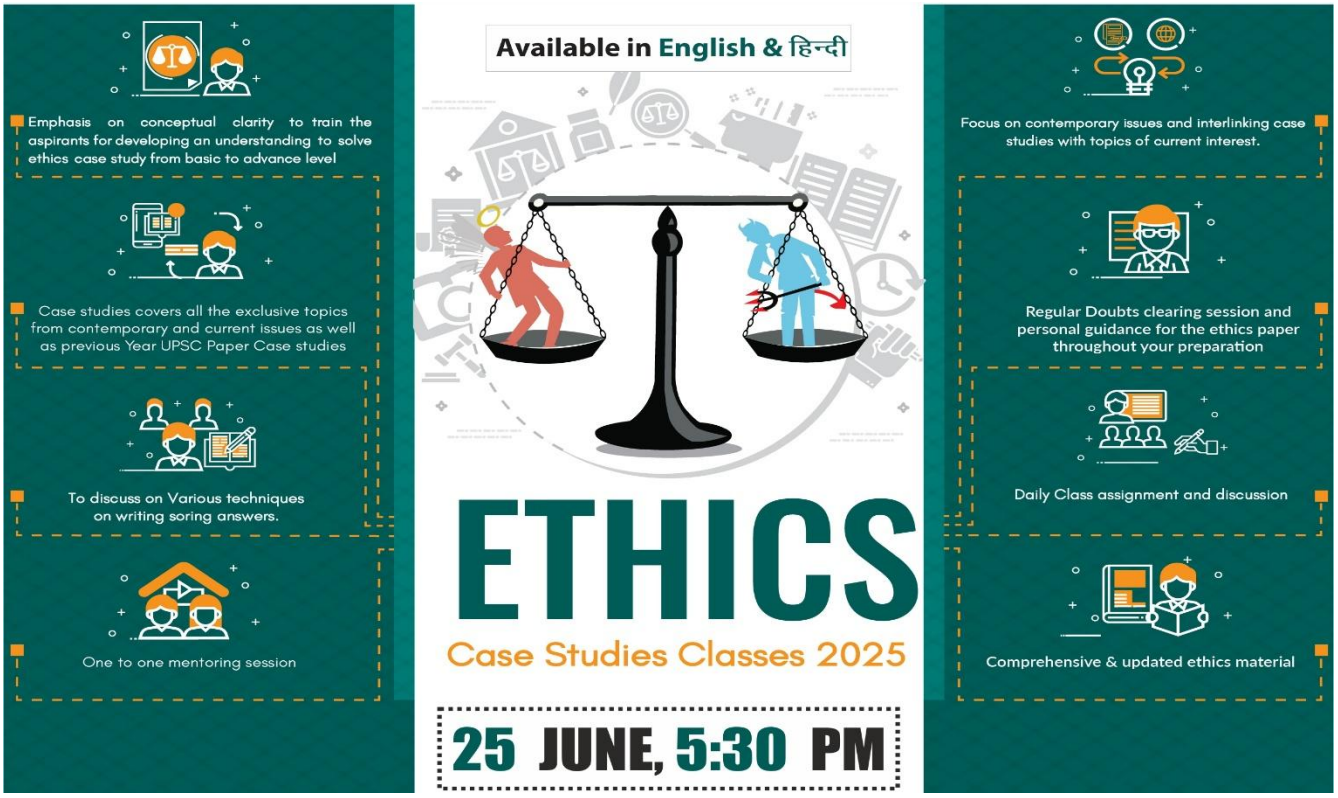
Money-laundering and its prevention

- Discuss how emerging technologies and globalization contribute to money laundering. Elaborate measures to tackle the problem of money laundering both at national and international levels. (2021 10 Marks)
- 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 10 Marks)

Security challenges and their management in border areas; Linkages of organized crime with terrorism, Various Security forces and agencies and their mandate

- Discuss the types of organised crimes. Describe the linkages between terrorists and organised crime that exist at the national and transnational levels (2024, 10 marks).
- 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, 10 marks).
- 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 (2025 15 Marks).
- What are the maritime security challenges in India? Discuss the organisational, technical and procedural initiatives taken to improve the maritime security (2022, 10 marks).
- Analyse the complexity and intensity of terrorism, its causes, linkages and obnoxious nexus. Also suggest measures required to be taken to eradicate menace of terrorism. (2021 15 Marks)
- For effective border area management, discuss the steps required to be taken to deny local support to militants and also suggest ways to manage favourable perception among locals. (2020 10 Marks)
- Analyse internal security threats and transborder crimes along Myanmar, Bangladesh and Pakistan borders including Line of Control (LoC). Also discuss the role played by various security forces in this regard. (2020 15 Marks)
- 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 15 Marks)
- India's proximity to the two of the world's biggest illicit opium growing states has enhanced her internal security concerns. Explain the linkages between drug trafficking and other illicit activities such as gunrunning, money laundering and human trafficking. What counter measures should be taken to prevent the same? (2018 15 Marks)

- The scourge of terrorism is a grave challenge to national security. What solutions do you suggest to curb this growing menace? What are the major sources of terrorist funding? (2017 15 Marks)
- The terms 'Hot Pursuit' and 'Surgical Strikes' are often used in connection with armed action against terrorist attacks. Discuss the strategic impact of such actions. (2016 12.5 Marks)
- 'Terrorism is emerging as a competitive industry over the last few decades." Analyse the above statement. (2016 12.5 Marks)
- 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 12.5 Marks)
- Human right activists constantly highlight the view that the Armed Forces (Special Powers) Act, 1958 (AFSPA) is a draconian act leading to cases of human rights abuses by the security forces. What sections of AFSPA are opposed by the activists? Critically evaluate the requirement with reference to the view held by the Apex Court. (2015 12.5 Marks)
- "The diverse nature of India as a multi-religious and multi-ethnic society is not immune to the impact of radicalism which is seen in her neighbourhood." Discuss along with strategies to be adopted to counter this environment. (2014 12.5 Marks)
- 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 12.5 Marks)
- How does illegal transborder migration pose a threat to India's security? Discuss the strategies to curb this, bringing out the factors which give impetus to such migration. (2014 12.5 Marks)
- 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 Organization. What impact does this have on India's maritime security concerns? (2014 12.5 Marks)
- 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 12.5 Marks)
- 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 10 Marks)



7. APPENDIX: KEY DATA AND FACTS

Topics	Key Data and Facts
Left Wing Extremism (LWE)	• **Current Spread (2025):** 6 districts most affected, 18 Naxal-affected (down from 35 and 126 in 2014). • **Violence Reduction:** 81% reduction between 2010 and 2024. • **Reasons for Decline:** Strengthened Security (National Policy & Action Plan 2015, SAMADHAN Strategy), Developmental initiatives (178 Eklavya Model Residential Schools), Community Engagement (Civic Action Programme).
Insurgency in Northeast	• **Reasons:** Ethnic rivalries (Meitei vs Kukis), alienation (AFSPA), territorial conflicts, porous borders. • **Peace Initiatives:** Peace deals (NLFT, Bodo, Karbi Anglong Accords), Strategic Connectivity (UDAN, Rail upgrades), Infrastructure (National Sports University, AIIMS), Cultural Connect (Moidams of Choraideo, Ashtalakshmi Mahotsav).
Armed Forces Special Powers Act (AFSPA) 1958	• **Powers:** Armed forces can open fire, arrest/search without warrant, immunity from prosecution (with Central Govt. sanction). • **Applicability:** Parts of Assam, Manipur, Nagaland, Arunachal Pradesh. • **Recommendations:** Justice B.P. Jeevan Reddy Committee (2004) to scrap; Santosh Hegde Committee (2013) to review every six months.

Technology and Internal Security	• **Online Radicalisation:** Driven by growing internet access, fast spread of extreme ideas.
	  ○ Facilitating Factors: Echo Chambers, Micro-Targeting, Cybercrime/Terror Financing.
	  ○ Indian Initiatives: IT Act 2000 (blocking harmful content), I4C & MeitY (monitoring URLs).
	• **Social Media Influencers & National Security:** Influencers can spread fake news, foreign narratives, incite violence, promote secessionism, and aid terror propaganda.
	  ○ **Indian Laws:** Official Secrets Act 1923, Bharatiya Nyaya Sanhita (BNS) Section 152, IT Act 2000 (Sec. 69A to block content), IT Rules 2021.
	• **Crypto Currency Hawala Nexus:** Bitcoin trading resembles hawala.
	  ○ **Concern:** Enables money laundering, terror financing, tax evasion; hard to trace due to anonymity features.
	  ○ **Way Forward:** Global cooperation (UN Global Programme against Money Laundering), strong regulations (FATF, EU's MiCA).
	• **Quantum Computing in National Security:**
	  ○ **Impact:** Could break current encryption, enhance intelligence/ surveillance (SIGINT), optimize military logistics, enable economic warfare (IP theft).
	  ○ **India's Steps:** National Quantum Mission, QuEST Program, IIT Madras Centre for Quantum Computing (CQuICC).

Data Protection	• **Digital Personal Data Protection Act (DPDP) 2023:** Establishes framework for protection/processing of personal data.

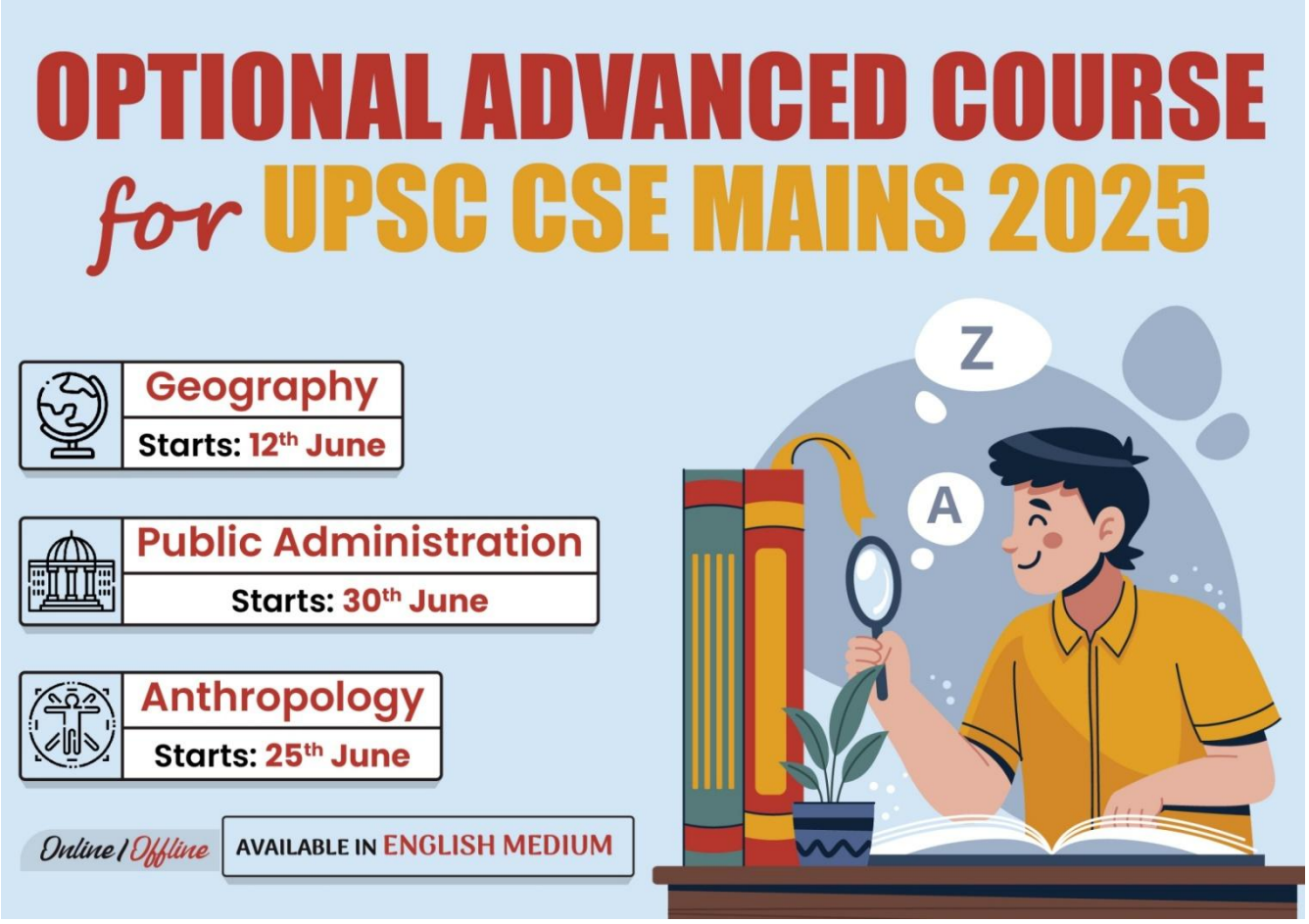
	○ **Key Features:** Consent-based, establishes Data Protection Board of India (DPBI), rights/duties for data principals, obligations for fiduciaries. ○ **Issues:** Broad state exemptions, missing data portability/right to be forgotten, weak board independence. • **Interception in India:** Telecommunications (Procedures and Safeguards for Lawful Interception of Messages) Rules, 2024. ○ **Legal Basis:** Telecommunication Act 2023, IT Act 2000 (Sec. 69). ○ **Concerns:** Broad definitions, vague terms ("public emergency"), concentration of power in executive, indefinite data retention. • **Facial Recognition Technology (FRT):** ○ **Risks:** Bias/misidentification (women, darker skin tones), privacy/security threats (hacking, misuse), lack of accountability. ○ **NITI Aayog Recommendations:** Privacy & Security, Governance Framework, Ethical Oversight.
Cyber Security	• **Need:** Weaponisation of Internet (India 2nd largest user base), strategic importance of cyberspace, emerging technologies (AI, ML), tackling cyberspace warfare, protecting vulnerable sections, and Critical Information Infrastructure (CII) • **Mechanisms:** Joint Doctrine for Cyberspace Operations (2024), National Cyber Security Policy, IT Act 2000, CERT-In, NCIIPC, I4C. • **Challenges:** Transboundary nature, funding, lack of national comprehensive architecture, data colonialism.
Geospatial Data & National Security	• **Significance:** Enhances intelligence/surveillance, situational awareness, military operations, crime prediction. • **India's Capabilities:** National Geospatial Policy 2022, EOS-07 satellites, NAVIC, Bharatmaps, Bhuvan, PM Gati Shakti, SVAMITVA.
Money Laundering (ML)/ Terror Financing (TF)	• **Money Laundering (ML)** is the **process of making illegally-gained proceeds** appears legal. • **Terrorist Financing (TF)** encompasses the **means** used by terrorist organizations to finance their activities. • **Challenges in Tackling ML/TF Weak enforcement** (69% of countries show major gaps, ED's conviction rate under PMLA is just 4.6%),**Delayed trials Virtual Digital Assets (VDAs)** allow anonymous, cross-border transfers. • **Way Forward**: **Enforce FATF Standards**, **Tackle crypto haven**, **International Cooperation**: (support conventions like **Palermo Convention** ,2000, **UNCAC**, 2003). **Adopt AI and blockchain** for tracking and tracing funds.
Drug Trafficking	• **Drug Trafficking:** Global increase (292 million users in 2022, +20% in 10 years). ○ **Threat:** National security (human trafficking, narco-terrorism), social crimes (youth addiction), institutional corruption, environmental damage. ○ **Challenge:** India is a "Transit Hub" between Golden Triangle and Golden Crescent. ○ **Indian Law:** Narcotics Drugs and Psychotropic Substances Act 1985.

Terrorism	• **India ranked 14th** on Global Terrorism Index 2025. • **Challenges:** No global definition of 'terrorism', state-sponsored terrorism (Pakistan), ineffective global cooperation, anonymity in terror financing. ○ **New Threats:** Hybrid & Virtual Terrorists, information warfare, emerging tech (drones, AI). • **Indian Counter-Terrorism:** UAPA 1967, NIA, NATGRID, India's New Security Doctrine (shift to "deterrence by punishment"), diplomatic Outreach against Pakistan's Sponsoring of Terrorism.
Transnational Organised Crimes (TNOCs)	• TNOCs **operate across borders** for financial/material benefit. • **Types:** drug/human/migrant trafficking, money laundering, cybercrime. • **Challenges:** Cross-border complexity, legal/policy gaps, economic inequality.

Border Security	• **India-China:** Disputes (Galwan, Aksai Chin, Doklam), inadequate infrastructure, water-sharing issues.
	• **India-Pakistan:** Disputes (Sir Creek, Kashmir), infiltration, cross-border terrorism (drones).
	• **India-Myanmar:** Drug trafficking (Golden Triangle proximity), porous border, insurgency.
	• **Kargil War (1999)**
	  ○ **Shortcomings (Kargil Review Committee):** Intelligence failure, low technology, defence underfunding, no clear security policy.
	  ○ **Reforms:** National Technical Research Organisation (NTRO), Multi Agency Centre (MAC), CDS created.
	• **Key Initiatives:** Comprehensive Integrated Border Management System (CIBMS), Border Infrastructure and Management (BIM) Scheme.

Maritime Security	• **Need:** Vulnerable coastline (26/11, piracy), geostrategic interests (net security provider), economic development (80% external trade through IOR). • **Post-26/11 Architecture:** Indian Navy, Coast Guard, BSF (creeks), CISF (ports), Sagar Suraksha Dal. • **Challenges:** Piracy/terrorism in IOR, maritime border disputes, Chinese influence, state govt. issues, environmental. • **Steps:** Coastal Surveillance (Sagar Kavach), Maritime Theatre Command (proposed), Information Fusion Centre – Indian Ocean Region (IFC-IOR).
Defence Modernisation	• **Need:** Challenging strategic environment, inadequate equipment, rapidly changing warfare (hybrid, cyber). • **Challenges:** Budget allocation, slow decision-making, technological limitations (indigenization), stalled structural reforms. • **India's Steps:** "Year of Reforms" (2025), Defence Acquisition Procedure (DAP) 2020, ADITI, iDEX, Mission DefSpace, Mission Shakti (ASAT).
Defence Exports	• **Status (FY 2024-25):** ₹23,622 crore record high. Top 25 arms exporters, to >100 countries. • **Steps:** iDEX, Defence Export Promotion Scheme (DEPC), Defence Industrial Corridors (DICs), Liberalised FDI Policy (74% auto route).
Nuclear Weapons	• **Nuclear Weapons Arsenal:** SIPRI Yearbook 2024 highlights rise. India's arsenal: 180 warheads (more than Pakistan's 170).

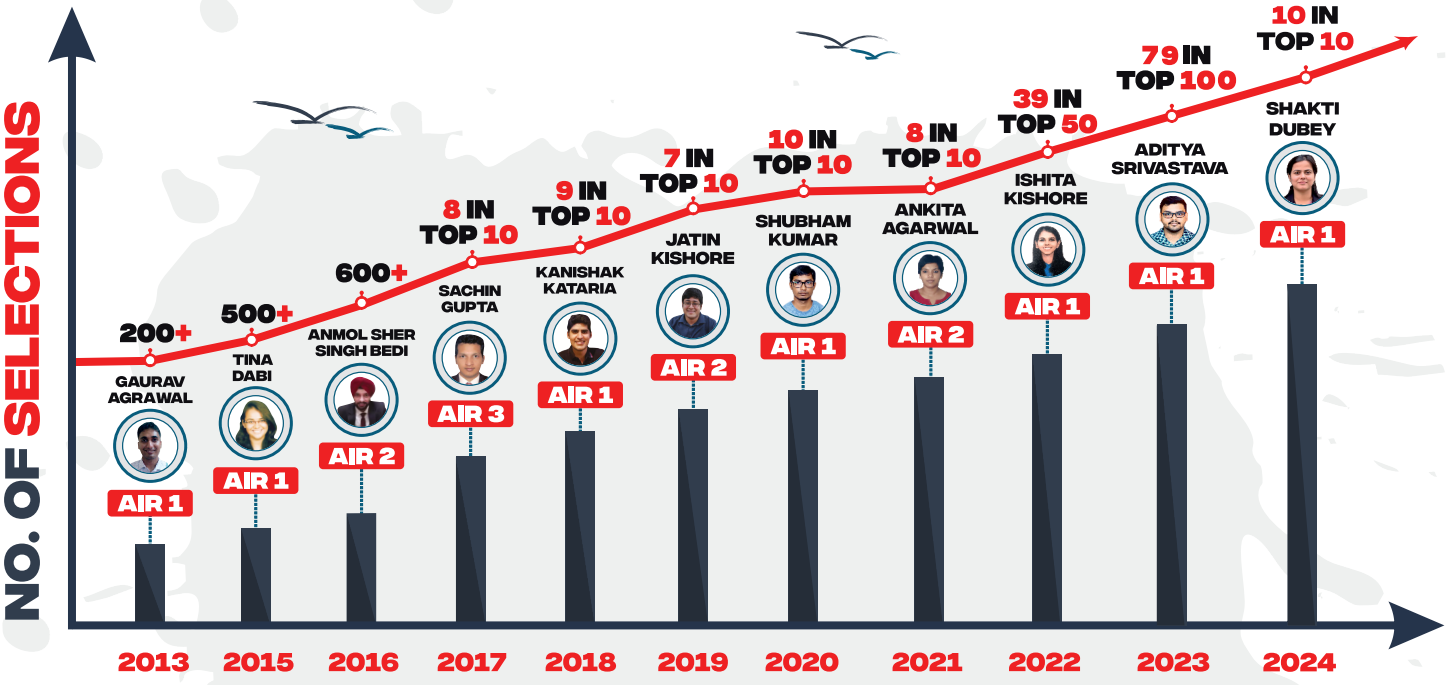
	○ **Threats:** Geopolitical tensions, risk of accidents, emerging tech (cyber, space-based nukes). ○ **Non-Proliferation:** IAEA, NPT (India, Israel, Pakistan not joined), CTBT (India not signed). • **India's Nuclear Doctrine (25 Years):** Launched 1999, formalized 2003. ○ **Key Features:** Credible Minimum Deterrence, No First Use (NFU), Massive Retaliation, No Use Against Non-Nuclear States, Disarmament support. ○ **Efficacy Debate of NFU:** Risk of initial casualties vs. strategic restraint.
Drones for Defense	• Drones used for ISR, precision attack, tactical edge. • **Concerns:** Weaponized drones, infrastructure disruption, overwhelming air defense (drone swarms). • **India's Counter-Drone:** Counter Drone System (D4), Bhargavastra.



Copyright © by Vision IAS
All rights are reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of Vision IAS.

VISIONIAS
INSPIRING INNOVATION

OUR ACHIEVEMENTS



LIVE/ONLINE
Classes Available
www.visionias.in

Foundation Course
GENERAL STUDIES
PRELIMS cum MAINS 2026, 2027 & 2028

DELHI : 8 JULY, 11 AM | 15 JULY, 8 AM | 18 JULY, 5 PM
22 JULY, 11 AM | 25 JULY, 2 PM | 30 JULY, 8 AM

GTB Nagar Metro (Mukherjee Nagar): 10 JULY, 8 AM | 29 JULY, 6 PM

हिन्दी माध्यम | 7 अगस्त, 2 PM

AHMEDABAD: 12 JULY | BENGALURU: 22 JULY | BHOPAL: 27 JUNE | CHANDIGARH: 18 JUNE
HYDERABAD: 30 JULY | JAIPUR: 5 AUG | JODHPUR: 2 JULY | LUCKNOW: 22 JULY | PUNE: 14 JULY

फाउंडेशन कोर्स सामान्य अध्ययन 2026

- प्रारंभिक, मुख्य परीक्षा और निबंध के लिए महत्वपूर्ण सभी टॉपिक का विस्तृत कवरेज

DELHI : 7 अगस्त, 2 PM | JAIPUR : 20 जुलाई | JODHPUR : 2 जुलाई

Scan the QR CODE to download VISION IAS App. Join official telegram group for daily MCQs & other updates.

/visionias.upsc | /c/VisionIASdelhi | /c/VisionIASdelhi | /t.me/s/VisionIAS_UPSC

DELHI: GMMR 33, Pusa Road, Near Karol Bagh Metro Station, Opposite Pillar No. 113, Delhi - 110005 CONTACT: 8468022022, 9019066066

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

Heartiest Congratulations

to all Successful Candidates

10 in **TOP 10** Selections in **CSE 2024**

from various programs of **Vision IAS**

1 AIR

Shakti Dubey

2 AIR

Harshita Goyal

GS Foundation Classroom Student

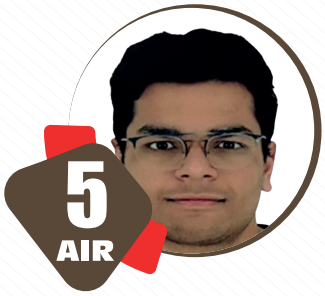
3 AIR

Dongre Archit Parag

GS Foundation Classroom Student

4 AIR

Shah Margi Chirag



5 AIR

Aakash Garg

6 AIR

Komal Punia

7 AIR

Aayushi Bansal

8 AIR

Raj Krishna Jha

9 AIR

Aditya Vikram Agarwal

10 AIR

Mayank Tripathi

79 Selections in **TOP 100** in **CSE 2023**

1 AIR

Aditya Srivastava

2 AIR

Animesh Pradhan

5 AIR

Ruhani

GMMR ENQUIRY & CLASSROOM CENTRE
33, Pusa Road,
Near Karol Bagh Metro Station,
Opposite Pillar No. 113,
Delhi - 110005

DELHI

MUKHERJEE NAGAR CENTER
Plot No. 857, Ground Floor,
Mukherjee Nagar, Opposite Punjab
& Sindh Bank, Mukherjee Nagar

GTB NAGAR CENTER
Classroom & Enquiry Office,
above Gate No. 2, GTB Nagar
Metro Building, Delhi - 110009

FOR DETAILED ENQUIRY
Please Call:
+91 8468022022,
+91 9019066066

enquiry@visionias.in /c/VisionIASdelhi /visionias.upsc /vision _ias VisionIAS_UPSC

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