VISIONIAS
INSPIRING INNOVATION

# SECURITY

Classroom Study Material 2021

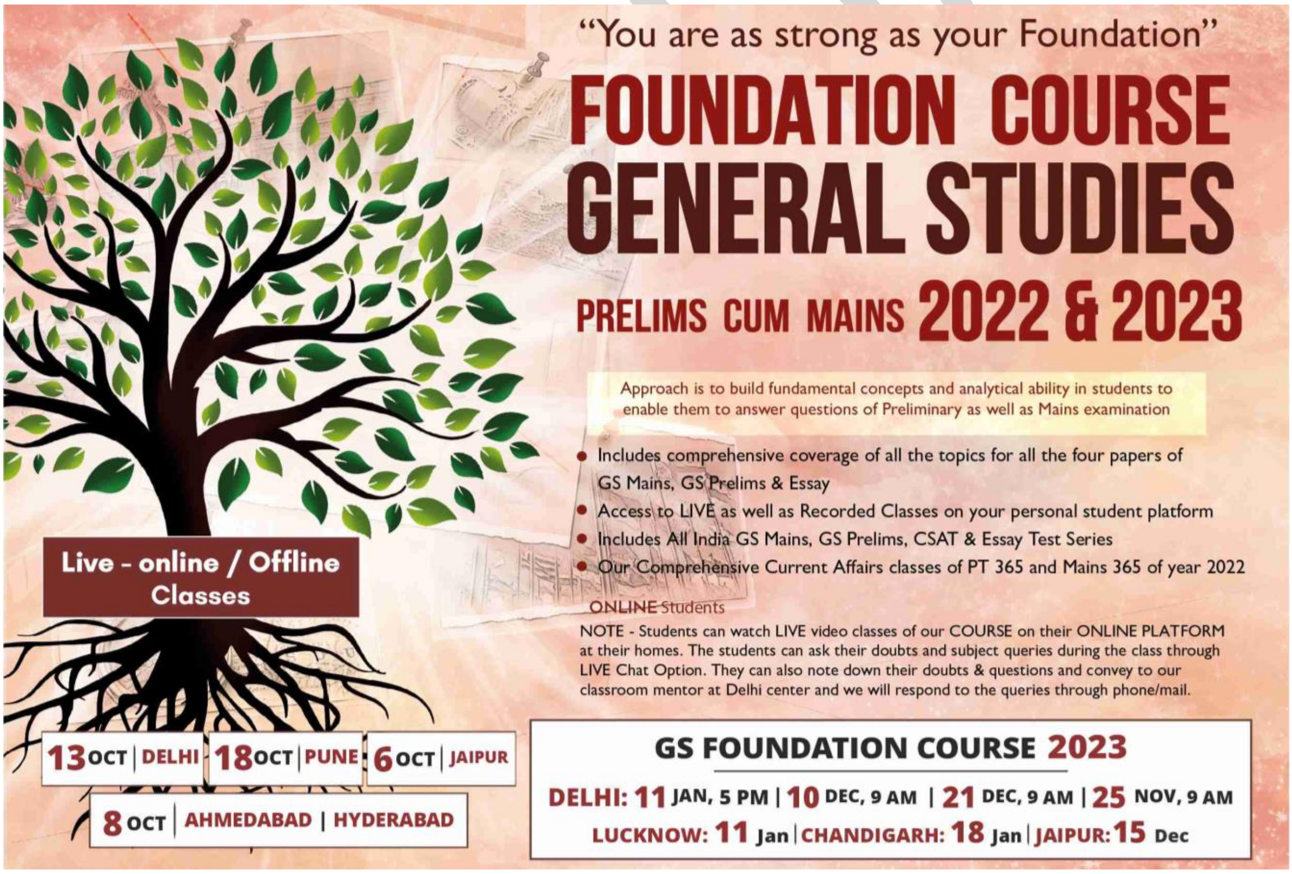
(September 2020 to September 2021)

www.visionias.in
+91 8468022022

DELHI | JAIPUR | PUNE | HYDERABAD | AHMEDABAD | LUCKNOW | CHANDIGARH | GUWAHATI

# SECURITY

## Table of Contents



Previous Year Questions

A reference sheet of syllabus-wise segregated previous year questions from 2013-2020 (for the Security Section) has been provided. In conjunction with the document, it will help in understanding the demand of the exam and developing a thought process for writing good answers.

# A NOTE FOR THE STUDENTS

*Dear Students,*

Every year with Mains 365 documents, we aim to provide consolidated content keeping in mind the demand of the exam and the corresponding needs of the students. This necessitates keeping pace with changing pattern of the examination.

Over the course of last 3-4 years, the nature of questions in the Mains examination has changed significantly. Questions are becoming more conceptual, and more holistic in nature (i.e., having an amalgamation of both static and current parts), for e.g. the question on local support and border management, in Mains 2020 examination.

**In this context we have made following additions in the document:**

- **Topic at glance:** Topic at glance have been added to the Mains 365 Security document. These topic at glance seek to:

Act as a bridge **connecting the static information** and the analysis of the current events.

Give a **360-degree view of the comprehensive topics** like Indigenisation of Defence Industry, Border Security etc.

Provide essential data/ initiatives related to the topic for **quick revision and replication in the examination.**

- **Infographics:** Infographics have been added in the document in a manner that they can readily be replicated in the examination through flowcharts, pie charts, maps etc., thereby improving the presentation of the content in the answers.

- **Previous year questions:** A QR code to the syllabus-wise segregated Previous Year Questions has been provided for student's reference. These will act as a guiding light for developing a thought process required for writing good answers.

The document seeks to not only provide a one stop solution for Security Current Affairs but it also seeks to develop a coherent thought process required for effective and well presented answer. Therefore, the articles in the document are not only to be read for content but also for understanding and adopting good practices of answer writing.

We hope that the coverage of the content in an organized manner will assist you in performing well in the examination.

Knowing is not enough; we must apply. Willing is not enough; we must do.

-Johann Wolfgang von Goethe

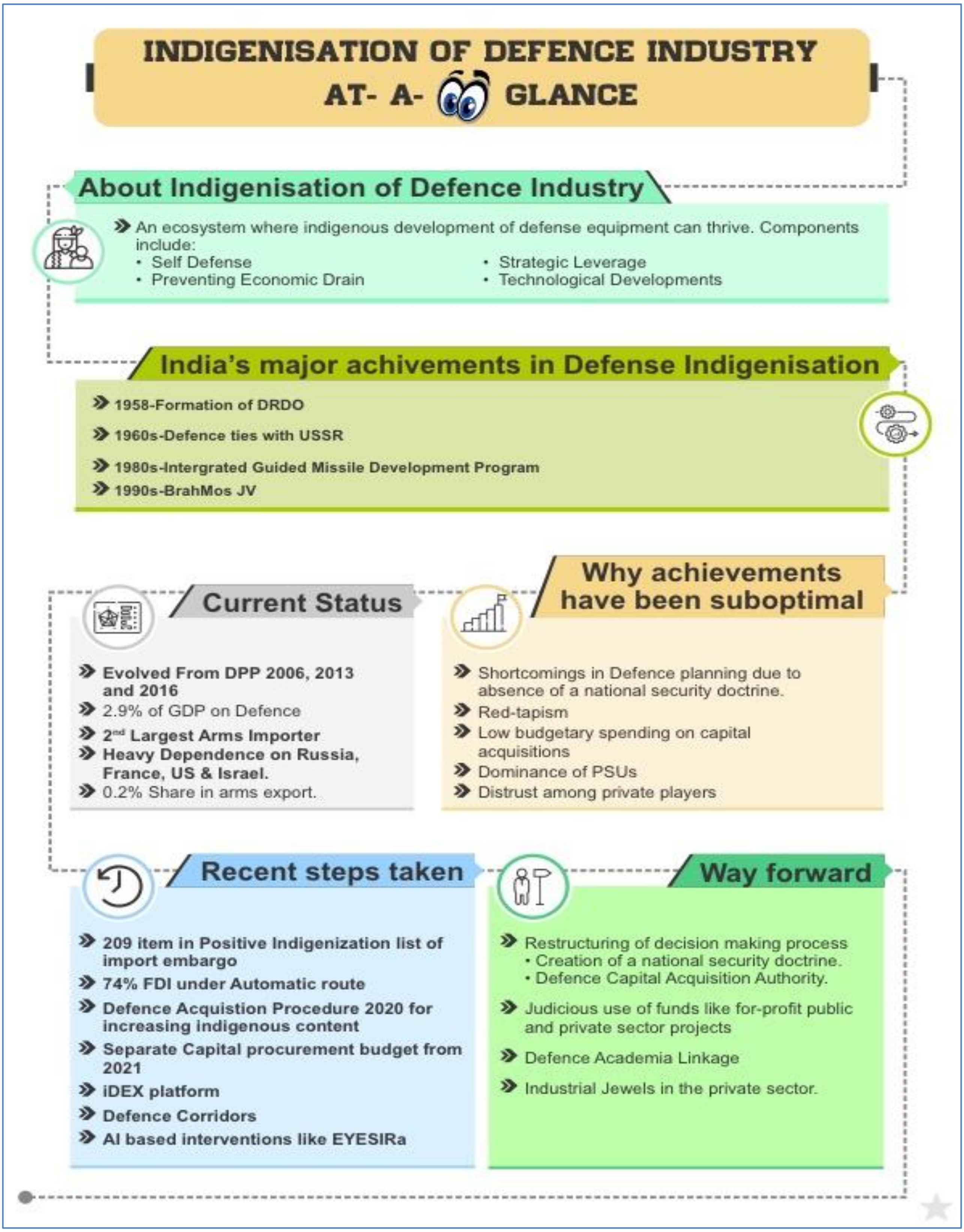
**All the best!**
**Team VisionIAS**

# 1. DEFENCE

## 1.1. INDIGENISATION OF DEFENCE INDUSTRY

**Why in news?**

With a series of measures to boost domestic defence industry, India was featured in the Stockholm International Peace Research Institute (SIPRI's) arms exporters list for the first time.



INDIGENISATION OF DEFENCE INDUSTRY AT- A- GLANCE

About Indigenisation of Defence Industry

- An ecosystem where indigenous development of defense equipment can thrive. Components include:
  - Self Defense
  - Preventing Economic Drain
  - Strategic Leverage
  - Technological Developments

India's major achivements in Defense Indigenisation

- 1958-Formation of DRDO
- 1960s-Defence ties with USSR
- 1980s-Intergrated Guided Missile Development Program
- 1990s-BrahMos JV

Current Status

- Evolved From DPP 2006, 2013 and 2016
- 2.9% of GDP on Defence
- 2nd Largest Arms Importer
- Heavy Dependence on Russia, France, US & Israel.
- 0.2% Share in arms export.

Why achievements have been suboptimal

- Shortcomings in Defence planning due to absence of a national security doctrine.
- Red-tapism
- Low budgetary spending on capital acquisitions
- Dominance of PSUs
- Distrust among private players

Recent steps taken

- 209 item in Positive Indigenization list of import embargo
- 74% FDI under Automatic route
- Defence Acquistion Procedure 2020 for increasing indigenous content
- Separate Capital procurement budget from 2021
- iDEX platform
- Defence Corridors
- AI based interventions like EYESIRa

Way forward

- Restructuring of decision making process
  - Creation of a national security doctrine.
  - Defence Capital Acquisition Authority.
- Judicious use of funds like for-profit public and private sector projects
- Defence Academia Linkage
- Industrial Jewels in the private sector.

Mains 365 - Security

## 1.1.1. DEFENCE ACQUISITION PROCEDURE, 2020

**Why in News?**

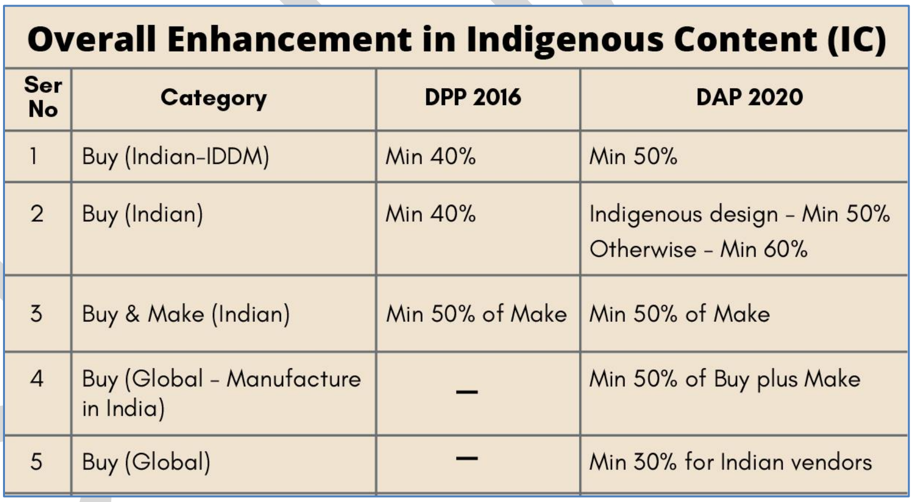
Recently Defence Ministry unveiled Defence Acquisition Procedure, 2020 (erstwhile Defence Procurement Procedure (DPP)) which will supersede DPP 2016.

**Significance of the policy**

- DAP is aligned with the vision of the government's 'Aatmanirbhar Bharat' **to make India a global defense manufacturing hub.**
- **Reduce dependence on imports:** India is one of the largest importers of conventional defence equipment spending about 30% of its total defence budget on capital acquisitions.
- **Boost overall economy:** Government aims for a turnover of ₹1.75 lakh crore in defence manufacturing by 2025.
- **Ensure timely acquisition of military equipment,** systems and platforms as required by the Armed Forces
- **To modernise and improve capabilities of the Armed Forces** by providing impetus to indigenisation and technology infusion.
- **Defined role for Private sector:** Private investment will be a major contributor to the 'Make in India' initiative, accelerate manufacturing-led industrial growth and for capital and technology advancement.

**Salient features of Policy**

- **To promote Indigenisation of Imported Spares:**
    - **List of Weapons/Platforms for Import Ban** to promote domestic and indigenous industry.
    - **New Category of Buy (Global – Manufacture in India)** has been incorporated in line with new FDI Policy and to encourage foreign original equipment manufacturers (OEMs) to setup 'manufacturing or maintenance entities' through its subsidiary in India while enabling requisite protections to domestic industry.
        - ✓ Recently there was enhancement of FDI through automatic route from 49% to 74% in defence.
    - **Request For Information(RFI) to** explore willingness of the prospective foreign vendors to setup an indigenous eco system at the spares/sub component level.
    - **Reservation in Categories for Indian Vendors:** The categories of Buy(Indian-IDDM), Make I, Make II, Production Agency in Design &Development, Ordinace Factory Board/DPSU and SP model will be exclusively reserved for Indian Vendors meeting the criteria of Ownership and Control by resident Indian Citizens with FDI not more than 49%.



**Overall Enhancement in Indigenous Content (IC)**

| Ser No | Category | DPP 2016 | DAP 2020 |
|---|---|---|---|
| 1 | Buy (Indian-IDDM) | Min 40% | Min 50% |
| 2 | Buy (Indian) | Min 40% | Indigenous design - Min 50%<br>Otherwise - Min 60% |
| 3 | Buy & Make (Indian) | Min 50% of Make | Min 50% of Make |
| 4 | Buy (Global - Manufacture in India) | – | Min 50% of Buy plus Make |
| 5 | Buy (Global) | – | Min 30% for Indian vendors |

    - **Other proposed measures such as** after sales support part of capital acquisition contract, higher indigenous content in acquisitions and incentives for local material and software and emphasis on product export under offsets.
- **For Time Bound Defence Procurement Process, Faster Decision Making and Ease of Doing Business:**
    - **Revision in Offset policy:** Offset policy clause (as there in the DPP 2002) for offsets for inter-government agreement (IGA), government-to-government defence deals and single-vendor contracts for the procurement of arms has been removed.
        - ✓ Under the offset policy, the foreign defence entities were mandated to **spend at least 30% of the total contract value in India** through procurement of components, transfer of technologies or setting up of research and development facilities.
    - **Setting up of project management unit (PMU) that** will facilitate obtaining advisory and consultancy support in specified areas to streamline the acquisition process and support contract management.
    - **Simplification of Trial Procedures to nurture competition.**
    - Single stage accord of **AoN (Acceptance of Necessity)** in all cases up to ₹500 crore to avoid delays in approval of acquisition proposals.
- **Leasing:** It has been introduced **as a new category for acquisition** in addition to the existing 'Buy' and 'Make' categories to substitute huge initial capital outlays with periodical rental payments.

  - This will be useful for military equipment not used in actual warfare like transport fleets, trainers, simulators, among others.
- **Strategic Partnership Model (SPM):** Acquisitions under the SPM refer to participation of private Indian firms along with foreign OEM in 'Make in India' in defense and play the role of a System Integrator by building an extensive eco-system comprising development partners, specialised vendors and suppliers, in particular, those from the MSME sector.
  - Strategic Partnerships will seek to enhance indigenous defence manufacturing capabilities through the private sector over and above the existing production base.

## 1.1.2. DEFENCE PROCUREMENT REFORMS

**Why in News?**

The Ministry of Defence approved '**Delegation of Financial Powers to Defence Services (DFPDS) 2021'** order, notifying enhanced delegation of Revenue Procurement powers to the Armed Forces.

**Why large share of imports?**

As per **Estimates Committee (2018)**, high dependence of armed forces on imports is due to-

- **Slow rate of indigenization.**
- **Limited indigenous capabilities,** especially on large and high-technology weapons/equipment necessary for modernization of defence forces.
- **Limited private sector** participation.

**More on News**

- Aimed to strengthen security infrastructure of the country through **greater decentralization**, it covers **Schedules of Powers** for **Army, Navy, Air Force,** and **Integrated Defence Staff.**
- The new guidelines devolve greater financial powers to field formations (5-10 times), Competent Financial Authorities (2 times), Vice Chiefs of Services (by 10%, subject to Rs 500 crore) etc.
- This includes up to **three times** increase in Schedules related to **Indigenization/R&D** to achieve 'Atma Nirbhar Bharat'.
- **Benefits for Armed Forces:** Streamlining of the procurement process for optimum utilization of resources; Meeting immediate necessities for better planning and operational preparedness; Quick decision making at all levels; and Greater integration among Services.

**Status of Defence Procurements by India**

- **Expenditure: India is the third largest military spender of world**, after USA and China, with a defence budget of about US$ 73 billion.
- **Distribution of expenditure:** Out of total expenditure, about 1/3rd is allocated for **capital outlay** which includes the defence procurement, i.e., the acquisition of defence equipment, systems, and platforms.
  - Of the defence procurement share, **almost half of the amount is spent on purchases from foreign suppliers,** making India the 2nd **biggest importer** of weapons after **Saudi Arabia** (SIPRI Fact Sheet on 'Trends in International Arms Transfers, 2020')**.**

Despite large spending on foreign procurement, India's Defence Preparedness with regard to arms and ammunition and key defence systems like aircraft carriers and fighter jets remains sub-optimal.

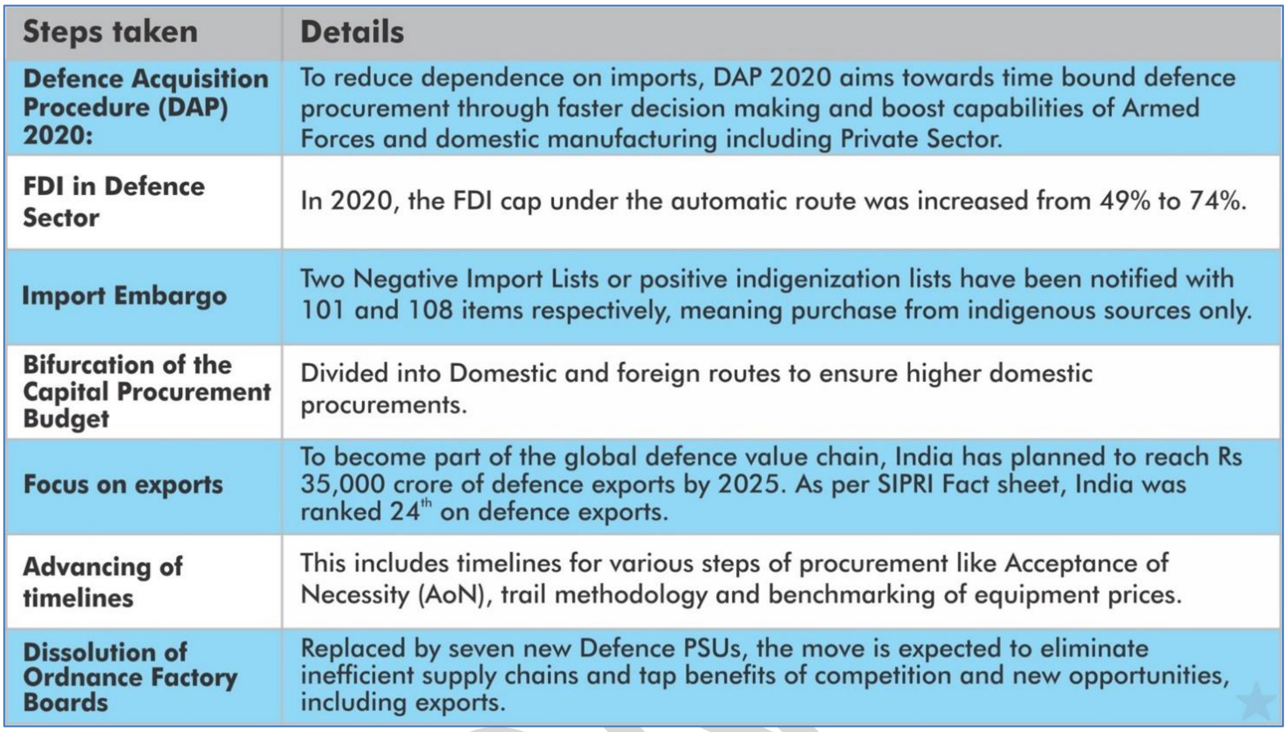
**What are the issues in Indian Defence Procurement ecosystem?**

- **Inordinate procedural delays**: The delay between projection of requirement by armed forces and actual delivery is quite high. E.g., the Submarine Project P-75I has reached only to Request for Proposal stage in 2021 despite being in pipeline for greater part of last two decades.
- **Coordination Issues**: Due to large number of stakeholders involved, the problem of coordination adds to the delay. For example, communication gaps between army and the Ministry of Defence.
- **Lack of Consistency**: Frequent changes in policy and specifications also cause delay or scrapping of projects. E.g., despite shortages and ageing assets, the old tenders issued through old policy are scrapped on adoption of a new policy.
- **Presence of corruption and middlemen:** Allegations of corruption and involvement of middlemen/vested interests are common in Indian defence procurements.
- **Political will:** Despite unsettled conflicts along borders, indecisive political decisions over foreign procurement has left armed forces severely ill-equipped.
- **Lack of strategic vision** on long-term defence needs in public domain, discouraging investments from foreign and domestic defence manufacturing.

The problems of procurement are accompanied by structural issues such as limited indigenization of the armed forces, limited and strained budgets among others.

**Steps taken to streamline overall Defence Procurement System**

While DFPDS provides for **operational efficiency**, steps are also taken to create a **robust procurement system.** From policy to actual production, following steps support faster and cheaper acquisition-



| Steps taken | Details |
|---|---|
| **Defence Acquisition Procedure (DAP) 2020:** | To reduce dependence on imports, DAP 2020 aims towards time bound defence procurement through faster decision making and boost capabilities of Armed Forces and domestic manufacturing including Private Sector. |
| **FDI in Defence Sector** | In 2020, the FDI cap under the automatic route was increased from 49% to 74%. |
| **Import Embargo** | Two Negative Import Lists or positive indigenization lists have been notified with 101 and 108 items respectively, meaning purchase from indigenous sources only. |
| **Bifurcation of the Capital Procurement Budget** | Divided into Domestic and foreign routes to ensure higher domestic procurements. |
| **Focus on exports** | To become part of the global defence value chain, India has planned to reach Rs 35,000 crore of defence exports by 2025. As per SIPRI Fact sheet, India was ranked 24th on defence exports. |
| **Advancing of timelines** | This includes timelines for various steps of procurement like Acceptance of Necessity (AoN), trail methodology and benchmarking of equipment prices. |
| **Dissolution of Ordnance Factory Boards** | Replaced by seven new Defence PSUs, the move is expected to eliminate inefficient supply chains and tap benefits of competition and new opportunities, including exports. |

**What can be done to further improve the Defence Procurement ecosystem?**

- **Early projection of Requirements:** Either through a **National Security Strategy** or other means, the defence establishments should articulate their medium to long-term requirement details. It will help in improving industry participation.
- **Accountability in Procurement:** Another main requirement is to fix responsibility for delays and corruption to bring accountability. This could be done by **simplifying procedures** through laying down clear processes with clear responsibilities.
- **Reduce stakeholders:** Setting up of a dedicated acquisition cell or dedicated cadre to look after procurements for all services will reduce coordination issues which cause delays.
- **Investments in Defence Production:** Being a capital-intensive industry with a long gestation period, the Defence PSU's and private sector requires government support through long-term projects and investments to create enabling infrastructure for R&D, testing of equipment etc. to create a **self-reliant defence ecosystem**.
- **Developing Defence-Industry-Academia linkage:** This linkage would create an ecosystem of defence innovation and research in the country resulting in decreased dependence of the country on foreign imports.

**Conclusion**

**Quick** and **transparent** defence procurement is **indispensable** to meet armed forces requirements to **ensure a secure India**. It will help in meeting challenges from **growing border tensions** and **rise of global terror outfits**. Also, it will strengthen the Indian defence ecosystem, boosting economic development through an efficient and accountable production system.

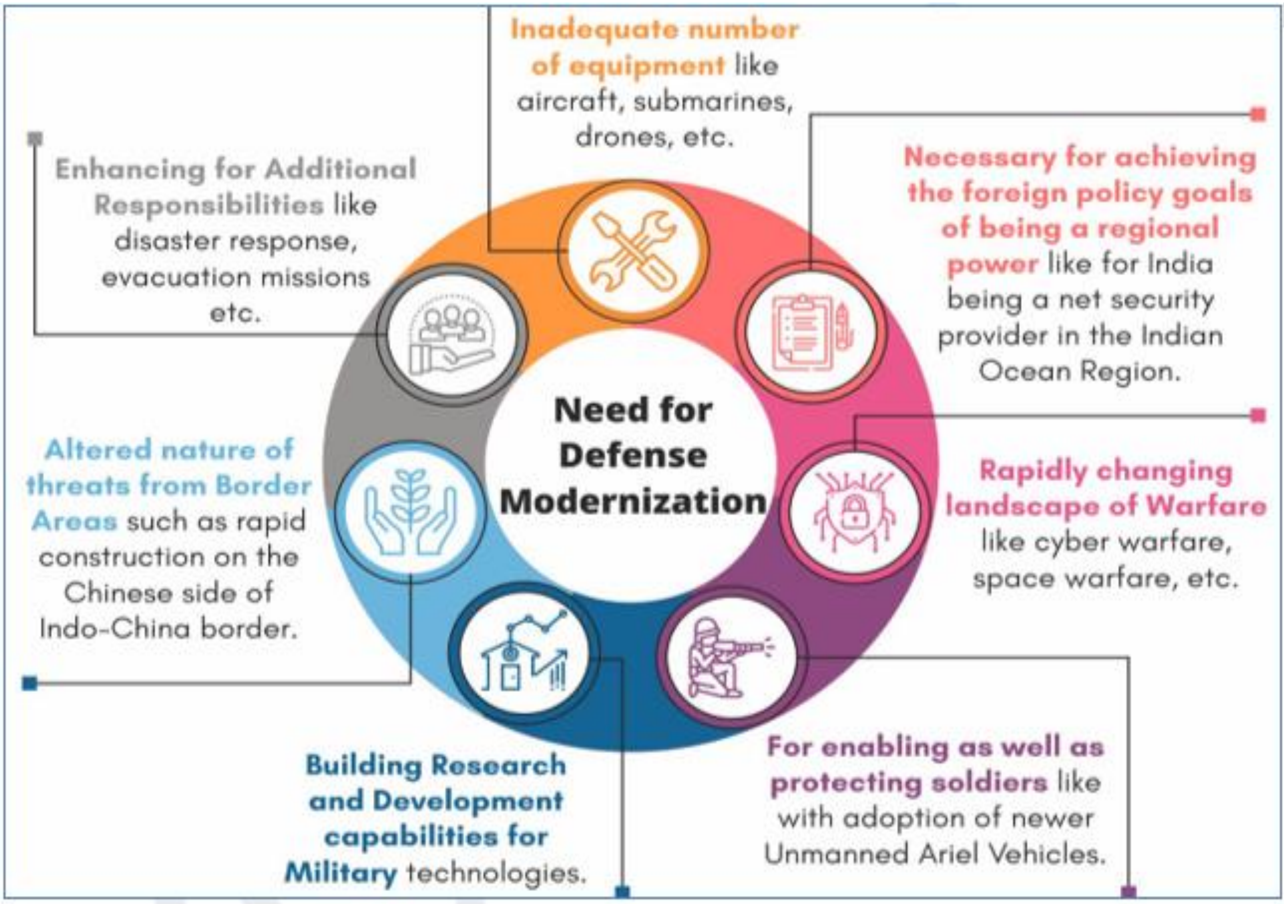
## 1.2. DEFENSE MODERNIZATION

**Why in News?**

The 15th Finance Commission has recommended constitution of a **dedicated non-lapsable Modernisation Fund** for Defence and Internal Security (MFDIS).

**More about the Fund**

- The primary aim of the Fund is to **bridge the gap between projected budgetary requirements and allocation** for defence and internal security.
- The indicative size of the **MFDIS for 2021-26 is about ₹2.5 lakh crore.**
- The Commission has recommended four specific sources of incremental funding which include :
  - transfers from the Consolidated Fund of India,
  - disinvestment proceeds of defence public sector undertakings (DPSUs),
  - proceeds from the monetization of surplus defence land, and
  - proceeds of receipts from defence land .
- The proceeds will be utilized for **capital investment for modernisation of defence services, Central Armed Police Forces (CAPF)** and **State police forces.**
  - The Fund would also allocate ₹1,000 crore per annum for the welfare of families of the defence and CAPF personnel who sacrifice their lives in frontline duties.


Need for Defense Modernization

Inadequate number of equipment like aircraft, submarines, drones, etc.

Necessary for achieving the foreign policy goals of being a regional power like for India being a net security provider in the Indian Ocean Region.

Rapidly changing landscape of Warfare like cyber warfare, space warfare, etc.

For enabling as well as protecting soldiers like with adoption of newer Unmanned Ariel Vehicles.

Building Research and Development capabilities for Military technologies.

Altered nature of threats from Border Areas such as rapid construction on the Chinese side of Indo-China border.

Enhancing for Additional Responsibilities like disaster response, evacuation missions etc.

**What are the steps that have been taken for defense modernisation?**

- **For defence production and indigenization:**
  - **Draft Defence Production and Export Policy 2020** with an aim to double India's defence production in five years.
  - **Defence Acquisition Procedure, 2020** aims to empower Indian domestic industry through 'Make in India' projects with the ultimate aim of turning India into a global manufacturing hub.
  - **SRIJAN Portal:** It is a **'one stop shop' online portal that provides access to the vendors** to take up items that can be taken up **for indigenization.**
  - **Encouraging Defence Entrepreneurship:** Organization of initiatives like Defense India Startup Challenge for creation of create functional prototypes of products/technologies relevant for national security.
- **For improving military organization:**
  - **Chief of Defence Staff (CDS)** was created to provide "effective leadership at the top level" to the three wings of the armed forces. This is addition to creation of **new Department of Military Affairs** for better management of military resources and procurement.
  - **Creation of Integrated Battle Groups:** IBGs are brigade-sized, agile, self-sufficient combat formations, which can swiftly launch strikes against adversary in case of hostilities.

  - **Theatre commands with tr-service capabilities:** The armed forces are envisaged to be reorganized in multiple Theatre commands in which all the three services will operate in a regionally integrated manner.
- **Other efforts:**
  - **Integrated Air Defence Weapon System (IADWS):** US has approved the sale of an IADWS to India. It will create a multi-layered missile shield over the National Capital Territory (NCT) of Delhi.
  - **Defence Testing Infrastructure Scheme:** Setting up of Defence Testing Infrastructure will provide easy access and meet the testing needs of the domestic defence industry.

**What are the challenges that remain?**

- **Large time taken for the decision-making process:** Experts have highlighted that despite multiple avenues available for procurement and development, production and acquisition contracts take close to **7 to 9 years for finalization before the production starts.**
  - This creates a mismatch between needs of the armed forces and availability of equipment. Also, elongated timelines lead to creation of a **lag between the manufactured technology and the state-of-the-art technology.**
- **Limited Public Sector Manufacturing Capacity and Capability:** Agencies like Ordnance Factories, DRDO, HAL etc. are limited and overburdened and is marred with several issues.
  - For example, program to indigenously manufacture a fleet of modern battle tanks, christened as future ready combat vehicle, is also not moving forward due to procedural delays.
- **Absence of a concrete Defense Industrial Base:** Participation of the private sector in Defense manufacturing has been limited. The primary reason for this can be attributed to absence of communication platforms between industry and defense.
  - Although efforts are being made in the form of creation of Defense Industrial Corridors (DIC) such as Tamil Nadu DIC, private sector participation in Defense production is still miniscule.
- **Absence of discourse on nature of future warfare:** Although several threats have been emerging like increasing cyberattacks, China's tilt towards hybrid warfare through informational superiority etc., clear plan or strategy for future development of such capabilities has not been created.

**Way Forward**

- **Change in ideology from being the major importer to major exporter:** Change in ideology would indirectly streamline the acquisition and production procedures. This will also necessitate partnership with private sector to contribute and complete the development-design-produce-export cycle.
- **Providing handholding to private sector** in the form of guaranteed procurement, joint development etc.
- **Development of Industry-defence-academia linkage** to strengthen research capabilities.
- **Looking at defence modernization in an integrated manner:** Defense modernization has to happen in conjunction with infrastructural modernization, growing human resource capabilities of the country etc. For example, shipbuilding industry and developed ports play a key role in development of naval systems like submarines.

## 1.3. INTEGRATED THEATRE COMMANDS

**Why in news?**

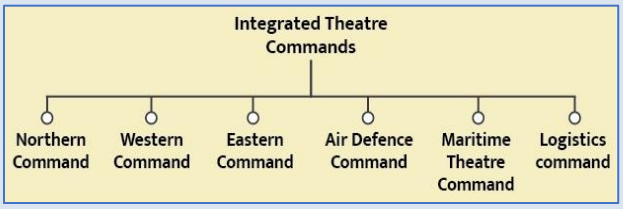
Recently, the Chief of Defence Staff (CDS) chaired a meeting with the Vice Chiefs of the three Services among others, in the backdrop of concerns about the proposed model of the Integrated Theatre Commands.

**Current system of military commands in India**

- Since 1947, the three services have been functioning separately and there has been proven cooperation between them but no integration per se.
- The **Indian Army, Navy and Air Force each has multiple commands that are vertically split** in terms of their command structure.
  - There are **17 military commands of tri-services,** seven of the Army and the Air Force each and three of the Navy, leading to **wastage and duplication of resources**.
- Apart from these, there are **two unified commands** i.e. Andaman and Nicobar Command (ANC) and the **Special Forces Command (SFC) for nuclear assets.**
- There are **four tri-service institutions** i.e. Defense Intelligence Agency, Defense Space Agency, Cyber Agency, and Armed Forces Special Operations Divisions, established in 2019.

**About Integrated Theatre Commands**

- An integrated theatre command envisages **a unified command of the three Services, under a single commander**, for geographical theatres that are of security concern.
  - The commander of such a force will be able to bring to bear all resources at his disposal — from the IAF, the Army and the Navy — with seamless efficacy.
- The idea of Integrated Theatre commands has been **proposed by both the Kargil review committee as well as D B Shekatkar committee.**
- The current theaterisation model under consideration seeks to set up **at least six new integrated commands.**
- India's **Chief of Defence Staff has been given the mandate to steer the theaterisation drive.**
- **Integrated Theatre Command in other countries**: More than **32 countries in the world already have** some form of theatre or joint command in place for better integration among the branches of the military. Notable among such countries are the US, China and Russia.



### Need for theatre commands

- **Changing nature of warfare:** Emerging forms of warfare such as hybrid, cyber and space warfare demands cooperation and synergy among the forces to achieve enhanced combat preparedness and interoperability between forces during peace.
- **Improved Resource efficiency:** The new model would reduce cost by cutting the duplication through optimum allocation and utilization of sources.
- **Better procurement:** Bulk purchase of military systems and equipment for the three services together would ensure cost reduction and strengthened leverage to the defense industry in India.
- **Quick decision making** in case of joint operations.
- **Reforms in the military capabilities of neighbouring countries such as China:** The possibility of an active Line of Actual Control (LAC), alongside of an already active Line of Control (LOC) has heightened in many ways the call for serious reforms in the Indian military.

### Challenges in implementing Integrated Theatre Commands

- **Geographical stretch of India:** Various experts have pointed that India is not geographically large enough to be divided into different theatres and the current model is sufficient to protect our territory and lanes of communication and is feasible in transportation.
- **Possibility of inter-service friction:** Some experts argue that this model would affect the independent service identity of forces and could lead to inter-service friction.
  - While the army and navy are in favour of theatre commands, the IAF has concerns about the model over the division of its air assets, dilution of powers of chiefs etc.
- **Limited domain knowledge and expertise of a theatre commander** could affect the functioning of command.
- **Operational hurdles:** Integrating the three services under the theatre command system faces hurdles like **who reports to whom** and how does the chain of command flow.
- **Financial constraints:** Budgetary allocations and the distribution of funds need to be clearly worked out to enable the setting up of a seamless theatre command system.

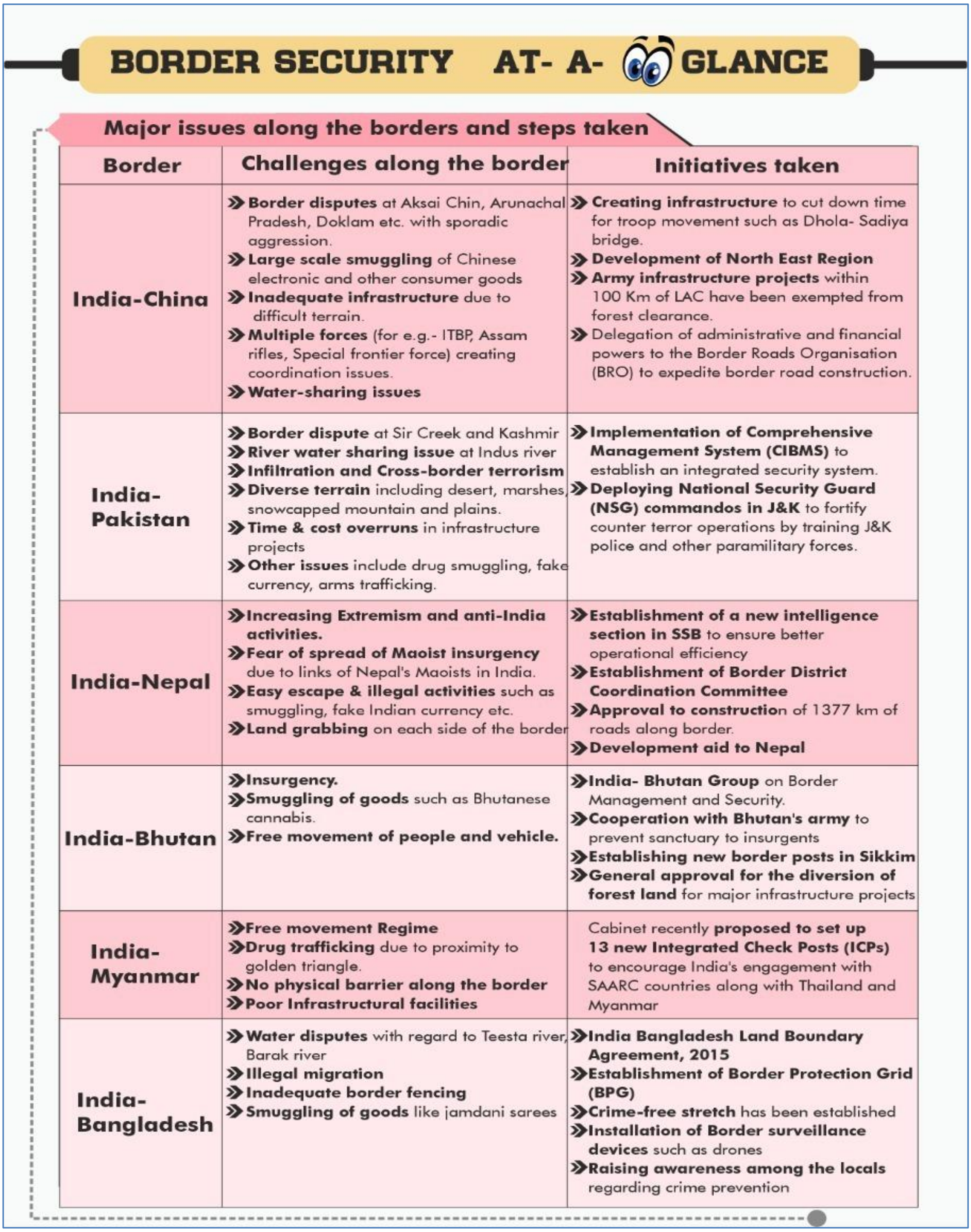
### Way ahead

- **Eliminating differences:** The government has formed an eight-member panel under the CDS to fine-tune the plans and bring all stakeholders on board.
- **Concurrence of the Ministry of Finance:** This is important as setting up of theatres and integration of various structures would have financial ramifications as well.
- **Streamlining decision making:** There is a need to decide who the theatre commanders would report to. For e.g. in the US the commanders report to the political leadership.
- **Other reforms through target intervention:** Steps should be taken to enable systems such as a robust and vibrant defence-industrial manufacturing complex, recognition of the changing nature of warfare, greater reliance on technological capabilities etc.

# 2. BORDER SECURITY AND MANAGEMENT

**Overview**

India has a land border of over 15,000 kms, which it shares with seven countries (Pakistan, China, Bangladesh, Nepal, Myanmar, Bhutan, and Afghanistan). Further, it has a coastline of over 7,500 kms. With largely **porous nature of border and other systemic issues**, it becomes important that we develop capabilities to protect our border areas in varied terrains, with multiple countries with whom we have very different security relationships.



BORDER SECURITY AT- A- GLANCE

Major issues along the borders and steps taken

| Border | Challenges along the border | Initiatives taken |
|---|---|---|
| India-China | » **Border disputes** at Aksai Chin, Arunachal Pradesh, Doklam etc. with sporadic aggression.<br>» **Large scale smuggling** of Chinese electronic and other consumer goods<br>» **Inadequate infrastructure** due to difficult terrain.<br>» **Multiple forces** (for e.g.- ITBP, Assam rifles, Special frontier force) creating coordination issues.<br>» **Water-sharing issues** | » **Creating infrastructure** to cut down time for troop movement such as Dhola- Sadiya bridge.<br>» **Development of North East Region**<br>» **Army infrastructure projects** within 100 Km of LAC have been exempted from forest clearance.<br>» Delegation of administrative and financial powers to the Border Roads Organisation (BRO) to expedite border road construction. |
| India-Pakistan | » **Border dispute** at Sir Creek and Kashmir<br>» **River water sharing issue** at Indus river<br>» **Infiltration and Cross-border terrorism**<br>» **Diverse terrain** including desert, marshes, snowcapped mountain and plains.<br>» **Time & cost overruns** in infrastructure projects<br>» **Other issues** include drug smuggling, fake currency, arms trafficking. | » **Implementation of Comprehensive Management System (CIBMS)** to establish an integrated security system.<br>» **Deploying National Security Guard (NSG) commandos in J&K** to fortify counter terror operations by training J&K police and other paramilitary forces. |
| India-Nepal | » **Increasing Extremism and anti-India activities.**<br>» **Fear of spread of Maoist insurgency** due to links of Nepal's Maoists in India.<br>» **Easy escape & illegal activities** such as smuggling, fake Indian currency etc.<br>» **Land grabbing** on each side of the border | » **Establishment of a new intelligence section in SSB** to ensure better operational efficiency<br>» **Establishment of Border District Coordination Committee**<br>» **Approval to construction** of 1377 km of roads along border.<br>» **Development aid to Nepal** |
| India-Bhutan | » **Insurgency.**<br>» **Smuggling of goods** such as Bhutanese cannabis.<br>» **Free movement of people and vehicle.** | » **India- Bhutan Group** on Border Management and Security.<br>» **Cooperation with Bhutan's army** to prevent sanctuary to insurgents<br>» **Establishing new border posts in Sikkim**<br>» **General approval for the diversion of forest land** for major infrastructure projects |
| India-Myanmar | » **Free movement Regime**<br>» **Drug trafficking** due to proximity to golden triangle.<br>» **No physical barrier along the border**<br>» **Poor Infrastructural facilities** | Cabinet recently **proposed to set up 13 new Integrated Check Posts (ICPs)** to encourage India's engagement with SAARC countries along with Thailand and Myanmar |
| India-Bangladesh | » **Water disputes** with regard to Teesta river, Barak river<br>» **Illegal migration**<br>» **Inadequate border fencing**<br>» **Smuggling of goods** like jamdani sarees | » **India Bangladesh Land Boundary Agreement, 2015**<br>» **Establishment of Border Protection Grid (BPG)**<br>» **Crime-free stretch** has been established<br>» **Installation of Border surveillance devices** such as drones<br>» **Raising awareness among the locals** regarding crime prevention |

### Steps that can be taken further

- **Dispute resolution-** Government should resolve pending border disputes with the neighbouring countries, as they later become matters of national-security threat.
- **No diversion of security forces-** The border-guarding force should not be distracted from its principal task and deployed for other internal security duties. For eg-ITBP, a force specifically trained for India-China border should not be used in the naxalite- infested areas.
- **Involvement of army –** It is felt that the responsibility for unsettled and disputed borders, such as the LoC in J&K and the LAC on the Indo-Tibetan border, should be that of the Indian Army while the BSF should be responsible for all settled borders.
- **Follow one-force-one-border principle** to effectively manage borders as divided responsibilities never result in effective control.
- **Developing Infrastructure-**accelerated development of infrastructure along the border, especially to wean the border population from illegal activities.
- **Denying local support to militants:** Integrating local community in border management and main streaming the youth by providing them education and employment opportunities.
- **Increasing use of technology** in border surveillance and management.

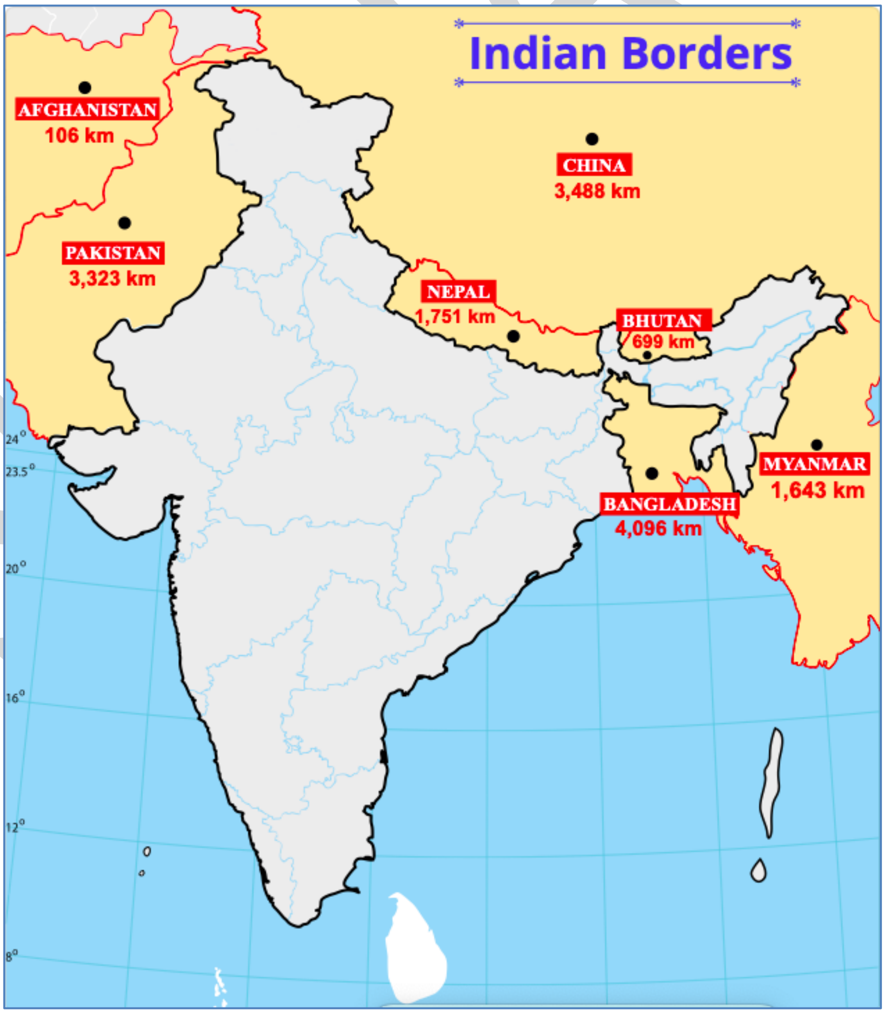
## 2.1. ROLE OF TECHNOLOGY IN BORDER MANAGEMENT

**Why in news?**

- Indian Army is working on converting the entire fence along **700 km stretch of Line of Control (LOC)** into **smart fence** to **improve surveillance and check infiltration.**

**More on news**

- The smart border fencing projects have been **built under the Comprehensive Integrated Border Management System (CIBMS)** programme along **Indo-Pakistan and Indo-Bangladesh** international borders.
- It has hi-tech surveillance system that would **create an invisible electronic barrier on land, water, air and underground.**
- The fence will be integrated with **LIDAR (Light Detection and Ranging) sensors, infrared sensors and cameras** among others and will **cost around ₹10 lakh per km.**

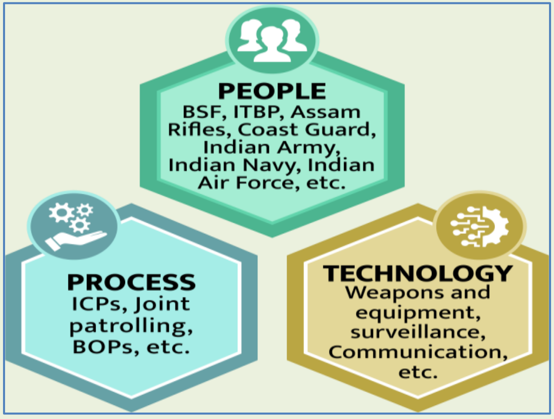


**Role of integrating technology in Border Management**

- **Complementing existing system:** At present, border guarding is almost fully dependent on human surveillance. This makes border management a time-consuming and complex task.
- **Checking infiltration:** It can be of help to detect infiltration via land, underwater, air and tunnels by deploying close circuit television cameras, thermal imagers and night vision devices etc.

- **Facilitate Cross Border Trade:** For example: Blockchain technology can help process transactions quickly and securely and makes identification and tracking of illegitimate trade easier.
- **Improved Intelligence inputs and Surveillance** through Remote sensing satellites, radar satellites and satellites with synthetic aperture radar (SAR) sensors which are capable of providing day and night all-terrain and all-weather inputs.
- **Madhukar Gupta Committee on border protection** had recommended the Union Government to **strengthen border protection and address vulnerabilities in fencing** along the Indo-Pakistan border. This led to **implementation** of **CIBMS in 2015**.

**Measures to respond to Border Management Challenges**


PEOPLE
BSF, ITBP, Assam Rifles, Coast Guard, Indian Army, Indian Navy, Indian Air Force, etc.
PROCESS
ICPs, Joint patrolling, BOPs, etc.
TECHNOLOGY
Weapons and equipment, surveillance, Communication, etc.

**Steps taken by the government to enable Technology driven Border Management**

- **Comprehensive Integrated Border Management System (CIBMS)**
  - It is a robust and integrated system that is capable of addressing the gaps in the present system of border security by seamlessly integrating human resources, weapons, and high-tech surveillance equipment such as thermal imagers, sensors, radars etc.
  - It **improves the capability of Border Security Force (BSF) in detecting and controlling the cross-border crimes** like illegal infiltration, smuggling of contraband goods, human trafficking and cross border terrorism etc.
  - It also **improves situational awareness** to facilitate prompt decision making and quick reaction to emerging situations.
  - In 2018, BSF undertook the **project BOLD-QIT** (Border Electronically Dominated QRT Interception Technique) to equip Indo-Bangladesh borders with different kind of sensors in unfenced riverine area of Brahmaputra and its tributaries.
- **Use of Space Technology to Secure India's Borders:** ISRO will launch a satellite exclusively for the use of the Ministry of Home Affairs, to help it further strengthen its frontiers both with Pakistan as well as Bangladesh, amongst several other countries.
- Recently, Government has approved a proposal for **the integration of communication and surveillance equipment to monitor activities on the Jammu border.**

### Challenges in deployment of technology in border areas

- **Infusion of large amount of fund** for acquiring the technology at a time when economy is struggling with slow growth.
- **Under-utilization of existing infrastructure**: The existing infrastructure in India's border areas, including detection, surveillance and communication technologies as well as physical structures is lying largely underutilized.
- **Lack of technical expertise**: The effectiveness of the technological equipment is further curtailed by the lack of training, repair and maintenance facility and smart users.
- **Adverse terrain**: Water bodies across borders create certain difficulties like changing course of the river, difficulty in detecting intrusions etc.
  - 12.36 percent of the Indo-Pakistan border is riverine, while 37 percent of the Indo-Bangladesh border is riverine.
  - Also, **erratic power supply** in such terrains hinders smooth working of technology.

### Way forward

- **Sharing financial burden:** A possible solution is to follow the **US–Mexico model**, where both the countries have jointly developed border areas, making them more stable economically, socially and demographically so that crime in the border areas can be minimized.
- **Capacity building**: Manpower must be trained before-hand and prompt service backup of equipment should be in place.
- **Private sector participation**: Efforts should be made to utilize the knowledge available with private sector in the context of electronic and surveillance equipment and maintenance and updating of data such as biometric details.

- **Continuous upgradation:** It is important to upgrade the present inventory of equipment and accessories in conjunction with the new project so that they are also utilized optimally.
- **Knowledge exchange and experience sharing** with international border-guarding forces can also be taken into consideration.

### Conclusion

One of the main aspects of national sovereignty is the **safety and security of states' borders**. If the borders are safe and stable only then can the country enjoy economic and social prosperity and technology play a key role in this border management.

## 2.2. MARITIME SECURITY

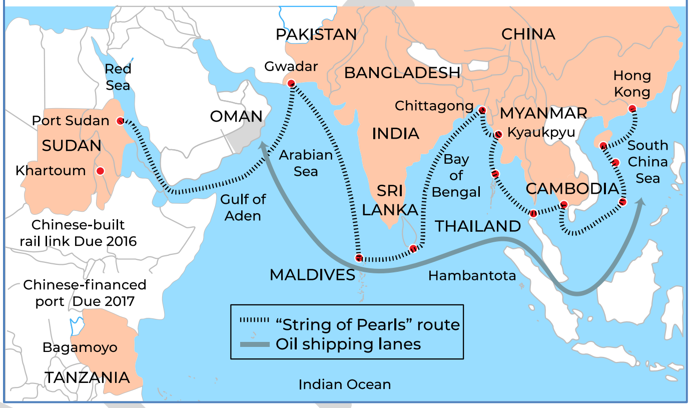
### Why in news?

India recently hosted the UNSC summit on maritime security where the UNSC adopted a 5 point agenda proposed by India for tackling maritime security.

### About Maritime Security

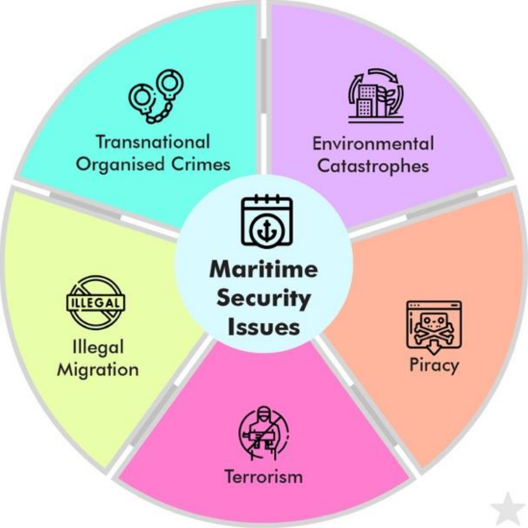
The term includes issues in the maritime domain comprising **national security, marine environment, economic development, and human security**. Besides the world's oceans, it also deals with regional seas, territorial waters, rivers, and ports.

India's Maritime Boundary



### Why India needs to focus on Maritime Security?

- **International Trade:** Securing sea lanes of communication is imperative for India's economic growth as the major portion of imports and exports is carried on through maritime waters.
- **Coastal Security:** India's 7000 km of coastline enhances its vulnerability to maritime threats as testified by the 2008 Mumbai attacks.
- **Chinese Assertion:** China's rising influence in the Indian Ocean region may threaten India's regional interest.
- **Harnessing blue economy:** The marine sector has immense future potential, but its development is possible only in a secure marine environment.
  - Economic activities dependent on marine resources, comprises 4.1% of India's economy.
- **Technological Developments:** Rapidly evolving nature of threats demands a greater focus on securing our marine environment.
  - For instance, an Israeli ship was attacked recently by a drone in the north Arabian Sea, killing two crew members.



### Issues in tackling maritime challenges

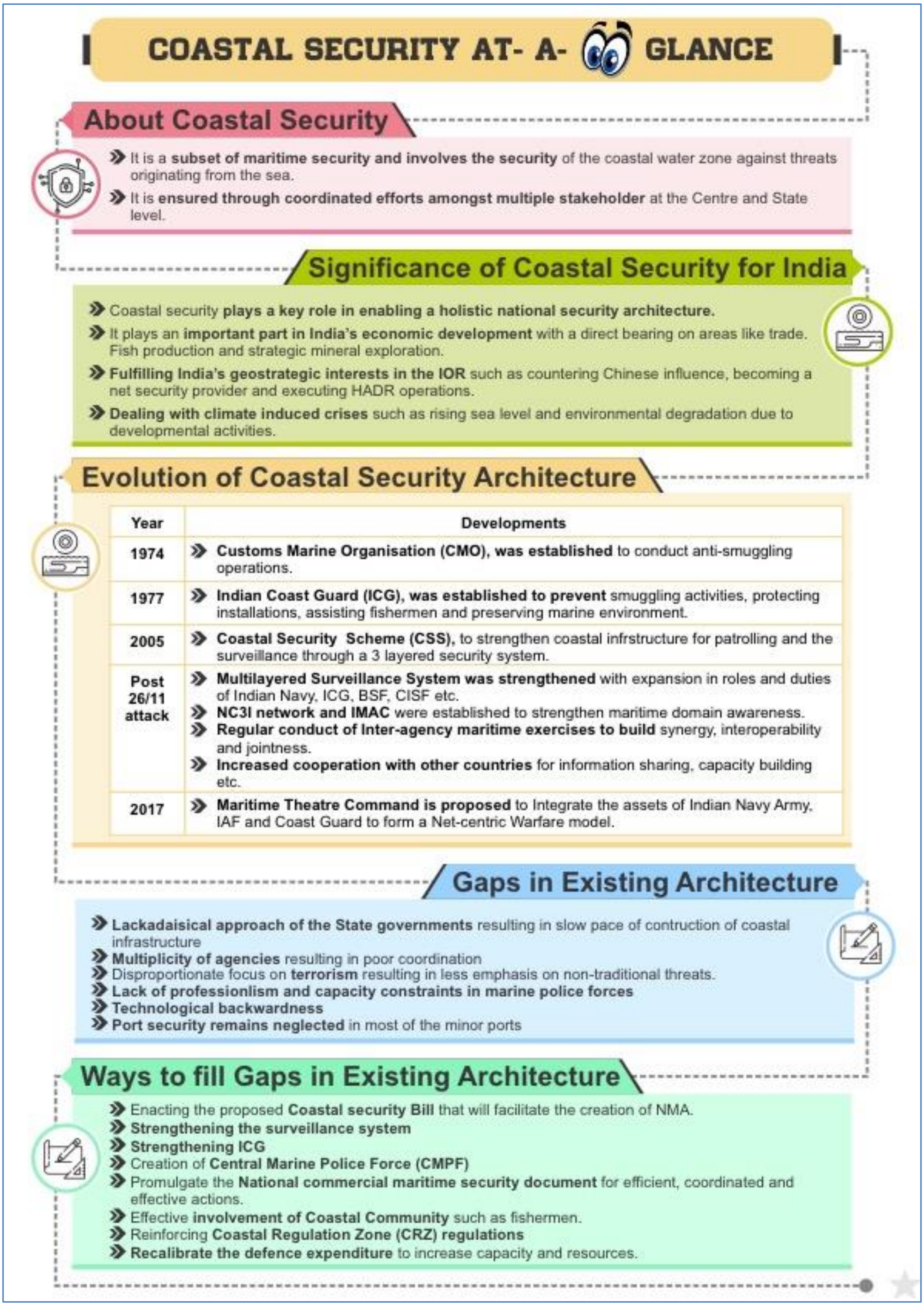
- **Disregard for the international law:** Strong nations are often seen as practicing Non-obedience.
  - For instance, China disobeyed the Permanent Court of Arbitration (PCA's) ruling that dismissed Beijing's claims on the entire area in the nine-dashed line in the South China Sea.
- **Maritime region is a global common:** As most of the maritime region is part of the high seas, no individual country can exercise sole jurisdiction over it. Therefore many countries refrain from investing their resources for augmenting the security framework. This peculiarity **enhances the vulnerability**.
- **International treaties lack universal character**: For instance, the US has only signed UNCLOS but not ratified it, thus generating scope for violation.
- **No Consensus on Definition**: Nations have failed to build a consensus over a uniform definition of maritime security.
- **Geopolitical Interests override Security Concerns**: For instance, Russia's geopolitical interests induce it to overlook China's violation of UNCLOS in the South China Sea region.

### Way forward

- **Adopting the 5 point agenda on maritime security:** The recently adopted 5 point agenda by UNSC should be implemented in letter and spirit. This includes:
    - Free maritime trade without barriers to establishing legitimate trade;
    - Settlement of maritime disputes should be peaceful and on the basis of international law only;
    - Responsible maritime connectivity should be encouraged;
    - Need to collectively combat maritime threats posed by non-state actors and natural calamities;
    - Preserve the maritime environment and maritime resources.
- **Building consensus on the creation of a maritime security body** in the UNSC, as proposed by the Russian President.
- **Universalising global treaties**: All the **countries must become part of Global treaties like UNCLOS** in order to foster better cooperation and coordination on maritime security. This would also **help in agreeing to a common definition** of maritime security.

**National and International mechanisms available to deal with maritime challenges**

- **Security and Growth for all in the Region (SAGAR):** Launched by India, the vision aims to deepen economic and security cooperation with India's maritime neighbours and assist in building their maritime security capabilities.
- **UN Convention on the Law of the Sea or the Law of the Sea Treaty (UNCLOS):** It defines the rights and responsibilities of all nations towards the use of the world's oceans.
- **Securing Indo-Pacific Region:**
    - **Indo-Pacific Oceans Initiative Partnership (AIIPOIP) :** An initiative under Australia-India partnership that will help shape maritime cooperation in the Indo-Pacific to support an open, inclusive, resilient, prosperous and rules-based maritime order.
        - ✓ The initiative **focused on seven pillars of maritime security** including Maritime Ecology, Disaster Risk Reduction and Management among others.
    - **QUAD**: An strategic dialogue between India, USA, Japan, and Australia where the objective is to ensure and support a "free, open, and prosperous" Indo-Pacific region.
- **Contact Group on Piracy off the Coast of Somalia (CGPCS):** It is an international governance mechanism to facilitate the discussion and coordination of actions among states and organizations to suppress Somali piracy.



# COASTAL SECURITY AT- A- GLANCE

## About Coastal Security

- It is a **subset of maritime security and involves the security** of the coastal water zone against threats originating from the sea.
- It is **ensured through coordinated efforts amongst multiple stakeholder** at the Centre and State level.

## Significance of Coastal Security for India

- Coastal security **plays a key role in enabling a holistic national security architecture.**
- It plays an **important part in India's economic development** with a direct bearing on areas like trade. Fish production and strategic mineral exploration.
- **Fulfilling India's geostrategic interests in the IOR** such as countering Chinese influence, becoming a net security provider and executing HADR operations.
- **Dealing with climate induced crises** such as rising sea level and environmental degradation due to developmental activities.

## Evolution of Coastal Security Architecture

| Year | Developments |
|---|---|
| 1974 | **Customs Marine Organisation (CMO), was established** to conduct anti-smuggling operations. |
| 1977 | **Indian Coast Guard (ICG), was established to prevent** smuggling activities, protecting installations, assisting fishermen and preserving marine environment. |
| 2005 | **Coastal Security Scheme (CSS),** to strengthen coastal infrstructure for patrolling and the surveillance through a 3 layered security system. |
| Post 26/11 attack | **Multilayered Surveillance System was strengthened** with expansion in roles and duties of Indian Navy, ICG, BSF, CISF etc.<br>**NC3I network and IMAC** were established to strengthen maritime domain awareness.<br>**Regular conduct of Inter-agency maritime exercises to build** synergy, interoperability and jointness.<br>**Increased cooperation with other countries** for information sharing, capacity building etc. |
| 2017 | **Maritime Theatre Command is proposed** to Integrate the assets of Indian Navy Army, IAF and Coast Guard to form a Net-centric Warfare model. |

## Gaps in Existing Architecture

- **Lackadaisical approach of the State governments** resulting in slow pace of contruction of coastal infrastructure
- **Multiplicity of agencies** resulting in poor coordination
- Disproportionate focus on **terrorism** resulting in less emphasis on non-traditional threats.
- **Lack of professionlism and capacity constraints in marine police forces**
- **Technological backwardness**
- **Port security remains neglected** in most of the minor ports

## Ways to fill Gaps in Existing Architecture

- Enacting the proposed **Coastal security Bill** that will facilitate the creation of NMA.
- **Strengthening the surveillance system**
- **Strengthening ICG**
- Creation of **Central Marine Police Force (CMPF)**
- Promulgate the **National commercial maritime security document** for efficient, coordinated and effective actions.
- Effective **involvement of Coastal Community** such as fishermen.
- Reinforcing **Coastal Regulation Zone (CRZ) regulations**
- **Recalibrate the defence expenditure** to increase capacity and resources.

### 2.2.1. PIRACY IN THE INDIAN OCEAN REGION

**Why in news?**

Recently, India has joined **Djibouti Code of Conduct/ Jeddah Amendment (DCOC/JA)** as an Observer.

**About Djibouti Code of Conduct**

- The DCOC, **established in 2009 under International Maritime Organization**, is aimed at **repression of piracy and armed robbery against ships** in the Western Indian Ocean Region, the Gulf of Aden and the Red Sea.
  - Jeddah Amendment significantly **broadened the scope of the Djibouti Code.** It covers measures for suppressing a range of illicit activities, including piracy, arms trafficking, trafficking in narcotics, illegal trade in wildlife, etc.
  - The members also cooperate in the **investigation, arrest and prosecution** of persons suspected of having committed acts of piracy, the **interdiction and seizure** of suspect ships, the **rescue of ships and people** subject to piracy and armed robbery, and the **conduct of joint operations.**
- It is a grouping on **comprising 18 member states** adjoining **the Red Sea, Gulf of Aden, the East Coast of Africa and Island countries** in the Indian Ocean Region.
- As an observer, India will be looking forward to working together with DCOC/JA member states towards **coordinating and contributing to enhanced maritime security** in the Indian Ocean Region.

**What is piracy, its associated threats and status in the Indian Ocean Region?**

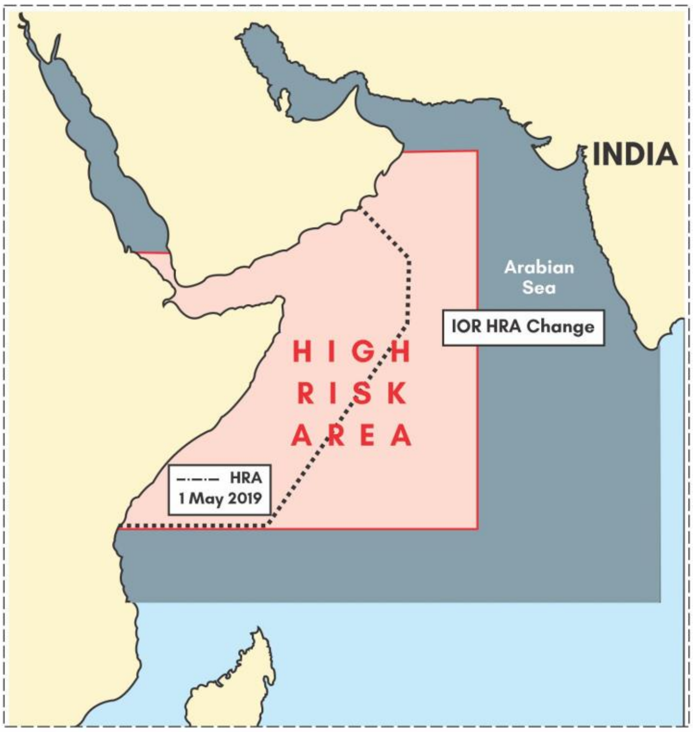
Under article 101 of UN Convention on the Law of the Sea, piracy is defined as: "Any acts **of violence, detention, or depredation committed on the high seas** by the crew or passengers of a private ship or aircraft against another ship, aircraft, persons, or property in a place outside the jurisdiction of any state for private ends."

**Rich pickings at sea**, **political instability**, the **lack of law enforcement and poverty** on land are major factors which have contributed to the increase in piracy. The issue of piracy manifests in the form of **hijacking of ships, with a focus on kidnapping and ransom payments**. This generates several threats such as-

- **Trade hinderance:** For example, Africa's sea Lanes of communications are affected adversely as over 90% of Africa's imports and exports are moved by sea.
- **Petro-Piracy:** Most of the **piracy intentioned attacks** have been against ships involved in **oil and gas transportation,** such as tankers, bulk carriers and tugs. For example, the coastline off Nigeria saw the most attacks in 2018 **targeting tankers from Nigeria's rich oil and gas fields.**

The piracy threat in the **Indian Ocean region** was **primarily recognized in 2008 by United Nations Security Council (UNSC) resolution for counter-piracy operations.** Since then, following developments have happened:

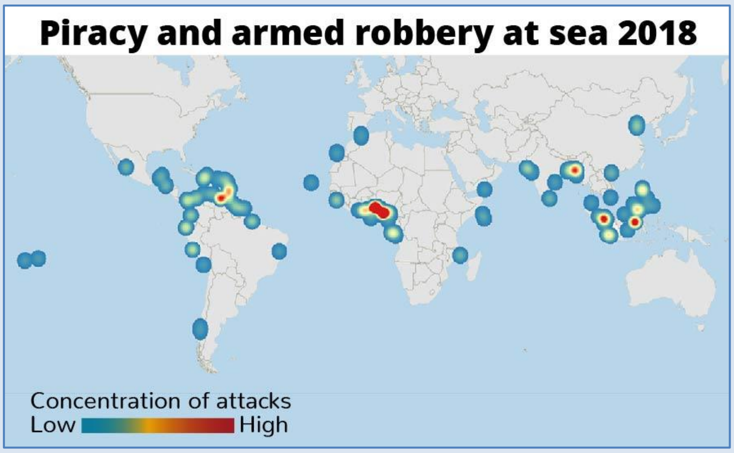
- The threat of piracy **peaked around 2011** when close to **160 major incidents were reported.**
- **Since 2013**, the number of **attacks and hijackings have significantly dropped**. For instance, in 2019, only two attacks were reported in the region.
- As a consequence of these decreased instances, the geographic boundaries of the **'High Risk Area' (HRA) for piracy in the Indian Ocean have been reduced.**
  - The High Risk Area reflects the area where the threat from piracy exists.
- Among the **seafarers affected from piracy** in this region, around **half are from the Philippines, followed by India, Ukraine and Nigeria.**



**Global Situation vis-a-vis privacy: One Earth Future Report**

**One Earth Future** produces a report stating the global annual State of Maritime Piracy. The 2019 report states that – "While attacks have been falling substantially in some regions of the world, in West Africa they've been on the rise and are now more frequent than anywhere else."

- In 2018, there were **112 piracy incidents in West African waters.**
- **In Asia, the Malacca Strait,** between Malaysia and Indonesia, **experienced a high number of attacks** in 2015. Concerted action by regional naval forces has reduced the problem there, but piracy still persists.
- **Attacks against shipping in the Caribbean** and **off the coast of Latin American have risen.** Venezuela in particular has become a hotspot for piracy particularly due to economic and political instability.



**What are the efforts made by the Indian Government to counter piracy in the region?**

A large percentage of **India's trade including oil and fertilisers**, passes through the Gulf of Aden **($50 Bn of Imports and $60Bn of Exports)**. The safety and unhindered continuity of maritime trade, through ships that use this route, is a primary national concern as it directly impacts our economy. In the light of this, following steps have been taken by the Government:

- **Escort and protection:** The Indian Navy commenced **anti-piracy patrols** in the Gulf of Aden from 2008.
  - **Indian Naval and Coast Guard ships have also been deployed** in piracy prone areas nearer the Indian coast. **Around 1000 plus ships of various nationalities have been escorted** and more than 40 piracy attacks prevented by Indian forces till date.
  - The Director General Shipping has launched a **web-based registration service to avail of the escort facility**.
- **Global coordination:** By participating in the multilateral for a setup to combat piracy.
  - India is an active participant of various mechanisms like **"Shared Awareness and De-confliction (SHADE)"** that have been established to **facilitate sharing of information.**
  - **India, Japan and China** (all three nations operate independently) have agreed to **coordinate patrols** thereby ensuring an effective and **optimum use of the combined maritime assets to escort ships**, especially in the Internationally Recommended Transit Corridor established for use by all merchant ships in the Gulf of Aden.

**What are the efforts made by the International community to counter piracy in the region?**

- **Contact Group on Piracy off the Coast of Somalia:** It was established in 2009 as a voluntary, ad hoc international forum to coordinate international efforts in the fight against piracy off the coast of Somalia.
- **Maritime Security Programme (MASE):** It is a European Union-funded programme to promote Maritime Security in Eastern and Southern Africa and Indian Ocean. Under MASE, the Indian Ocean Commission (IOC) has established a mechanism for surveillance and control of the Western Indian Ocean with two regional centres in Madagascar and Seychelles.
- **Maritime Crime Programme (MCP) - Indian Ocean:** The Indian Ocean team within the **United Nations Office on Drugs and Crime's (UNODC) Maritime Crime Programme** assists states in the Indian Ocean region to enhance and coordinate their efforts to combat maritime crime, with a **focus on criminal justice capacity building.** Following can be cited as its key facets:
- **Other important regional efforts:**
  - **African Union's Lomé Charter:** The African Charter on Maritime Security, Safety and Development in Africa, also known as the Lomé Charter, was signed in 2016 by **heads of state and governments of African Union (AU) member states.**
  - **Yaoundé Code of Conduct:** The document brings together **signatory nations from West and Central Africa** with an intention to cooperate to the fullest possible extent in the repression of **transnational organized crime in the maritime domain, maritime terrorism, IUU fishing, and other illegal activities.**

### Addressing the root cause: The way forward

In the recent past, there have been notable successes in counter-piracy efforts in the Indian Ocean Region. But the **root cause of piracy problem** i.e. poverty, lack of employment opportunities in Somalia's coastal communities, as well as a lack of legal, governance and maritime infrastructure **have not been adequately addressed**.

The long-term success of counter-piracy measures depends on a stable and unified Somali state. This can be achieved by:

- A more coherent regional effort to **address smuggling would help stop the money flow** that fuels these groups.
- **Capacity building of Somalia's Navy**, so that dependency on foreign navies and need for international support progressively decreases.
- **Comprehensive counter-piracy efforts must keep the pressure** on pirate groups while addressing the root causes that enable these networks to emerge.

**Learning from Puntland State of Somalia**

- Puntland has been successfully **fighting piracy since 2008.**
- Once a center of pirate activity, the federal state has taken proactive and effective counter-piracy measures like **establishing a maritime police force** – to drive away pirate groups and secure the coast.

**Related news: Global power scrambling in Indian Ocean**

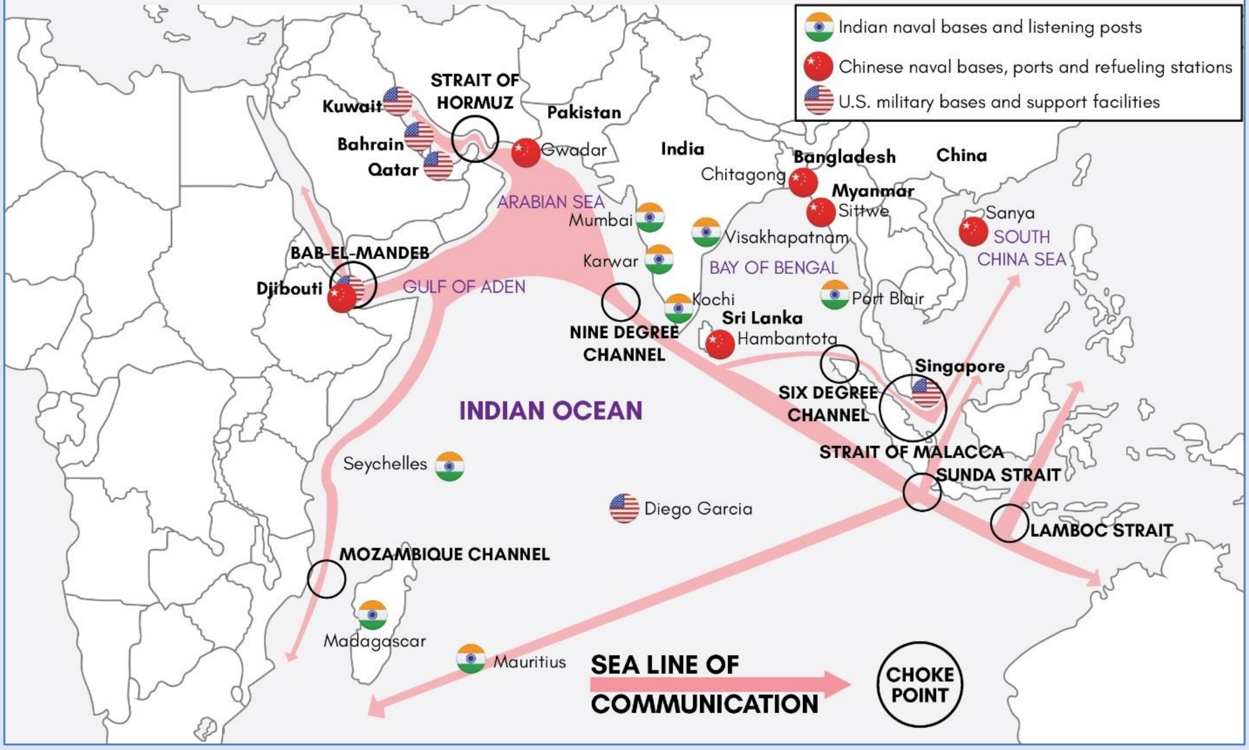
**IOR has become a pivotal zone of strategic competition.** There are more than 100 warships of extra-regional forces deployed in support of various missions. Global powers have shown a renewed interest in investing in infrastructure development in the IOR countries to maintain and increase geopolitical influence. Main reasons for this are:

- **IOR falls at the crossroads of global trade** with presence of important choke points such as Strait of Hormuz, Strait of Malacca etc.
- **Richness in natural resources such as oil, poly metallic nodules, fish etc.**
- **Ensuring global security as** more than half the world's armed conflicts are presently located in the IOR.
- **Countering rise of China**
- **Protection of maritime ecosystem**

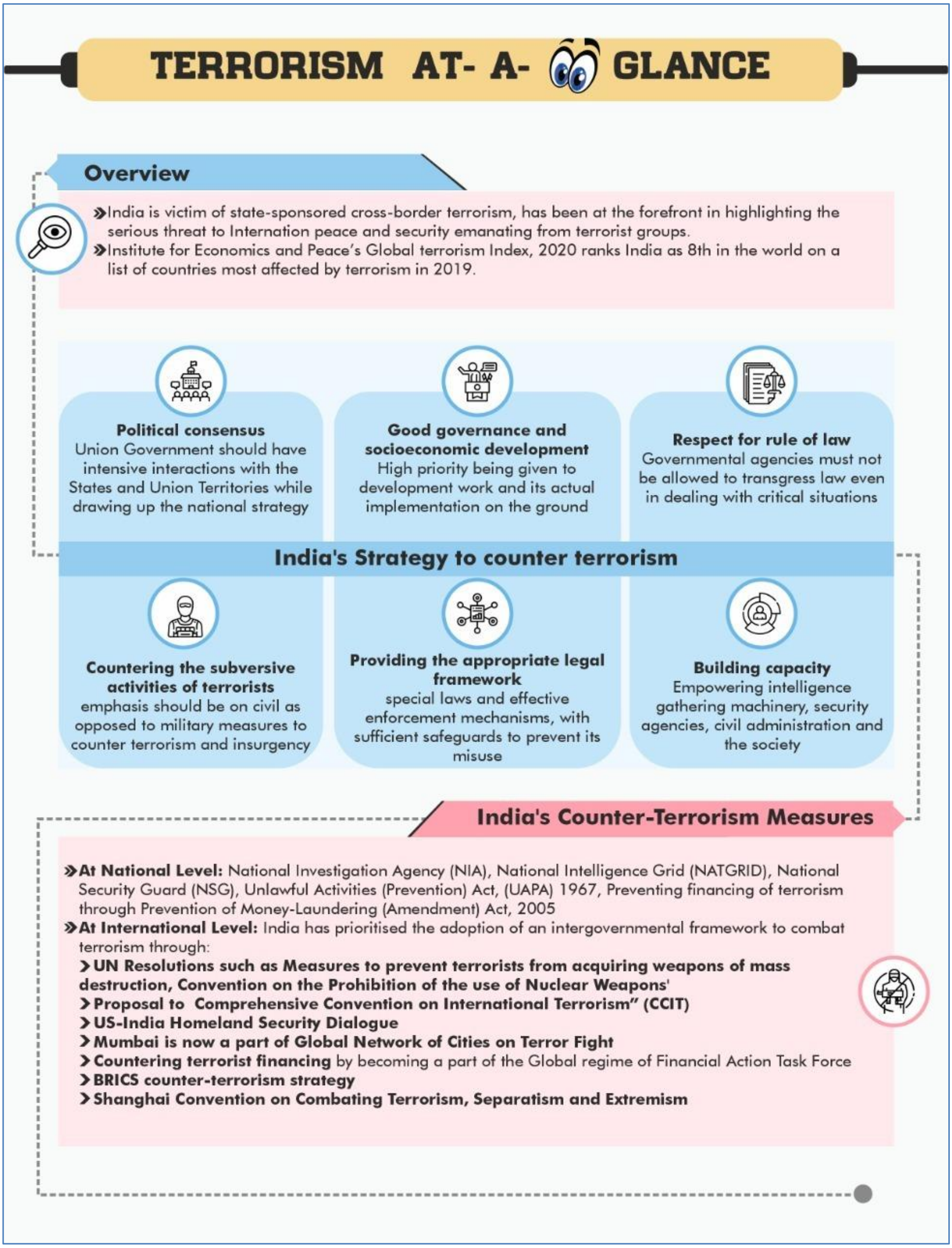
**How can India play a significant role in IOR?**

- **Maintaining strategic autonomy** by strengthening bilateral, trilateral and multilateral mechanism like 'JAI' (Japan, Australia, and India), India-ASEAN (Association of Southeast Asian Nations) and others.
- **Strengthening capability** through military logistics agreements such as LEMOA.
- **Improving regional connectivity and trade** by re-energizing SAARC, and finalising BIMSTEC FTA.
- **Cooperation with small littoral states** to prevent their tilt towards China

**Power balance in the Indian ocean**



# 3. TERRORISM



## TERRORISM AT- A- GLANCE

### Overview

- India is victim of state-sponsored cross-border terrorism, has been at the forefront in highlighting the serious threat to Internation peace and security emanating from terrorist groups.
- Institute for Economics and Peace's Global terrorism Index, 2020 ranks India as 8th in the world on a list of countries most affected by terrorism in 2019.

### India's Strategy to counter terrorism

**Political consensus**
Union Government should have intensive interactions with the States and Union Territories while drawing up the national strategy

**Good governance and socioeconomic development**
High priority being given to development work and its actual implementation on the ground

**Respect for rule of law**
Governmental agencies must not be allowed to transgress law even in dealing with critical situations

**Countering the subversive activities of terrorists**
emphasis should be on civil as opposed to military measures to counter terrorism and insurgency

**Providing the appropriate legal framework**
special laws and effective enforcement mechanisms, with sufficient safeguards to prevent its misuse

**Building capacity**
Empowering intelligence gathering machinery, security agencies, civil administration and the society

### India's Counter-Terrorism Measures

- **At National Level:** National Investigation Agency (NIA), National Intelligence Grid (NATGRID), National Security Guard (NSG), Unlawful Activities (Prevention) Act, (UAPA) 1967, Preventing financing of terrorism through Prevention of Money-Laundering (Amendment) Act, 2005
- **At International Level:** India has prioritised the adoption of an intergovernmental framework to combat terrorism through:
  - **UN Resolutions such as Measures to prevent terrorists from acquiring weapons of mass destruction, Convention on the Prohibition of the use of Nuclear Weapons'**
  - **Proposal to Comprehensive Convention on International Terrorism" (CCIT)**
  - **US-India Homeland Security Dialogue**
  - **Mumbai is now a part of Global Network of Cities on Terror Fight**
  - **Countering terrorist financing** by becoming a part of the Global regime of Financial Action Task Force
  - **BRICS counter-terrorism strategy**
  - **Shanghai Convention on Combating Terrorism, Separatism and Extremism**

## 3.1. UNLAWFUL ACTIVITIES [PREVENTION] ACT

### Why in news

Ministry of home affairs has stated that there was over 72% rise in number of UAPA (Unlawful Activities [Prevention] Act) cases in 2019 compared to 2015.

### About UAPA

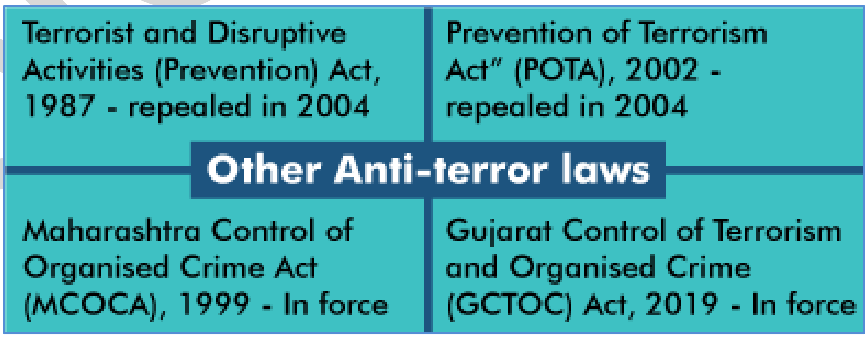
The Unlawful Activities (Prevention) Act, 1967 (Act) was enacted to **provide for more effective prevention of certain unlawful activities of individuals and associations,** and for **dealing with terrorist activities,** and related matters.

**Amendments to UAPA**

- **Amendments in 2004:** Criminalized indirectly supporting a terrorist organisation by raising of funds for a terrorist act or membership of a terrorist organization etc.
- **Amendments in 2008:** Broadened the scope of the provision of "funds" to ensure a wider coverage of the financing of terrorism offences.
- **Amendments in 2012:** Expanded the definition of "terrorist act" to include offences that threaten the country's economic security.
- **Amendments in 2019:**
  - Government is empowered to **designate individuals as terrorists**. Earlier, only organisations could be designated as terrorist organisations.
  - If investigation is conducted by an officer of the National Investigation Agency (NIA), **approval of Director General of NIA would be required for seizure of property connected with terrorism**. (Earlier, approval of Director General of Police was required).
  - **Empowered officers of NIA**, of rank of Inspector or above, to investigate cases.
  - Added International Convention for Suppression of Acts of Nuclear Terrorism (2005) to the Schedule under the Act.

**Provisions of the act:**

- **Act defines "Unlawful activity"** as "any action taken by individual or association that leads to **cession of a part of the territory of India, questions the sovereignty of India or disrupt the integrity of India** etc.
- **Powers with the government:**
  - Under the Act, Central government can **declare a person or an organization as a terrorist/ terrorist organisation**, if it/ he:
    - ✓ commits or participates in acts of terrorism,
    - ✓ prepares for terrorism,
    - ✓ promotes terrorism, or
    - ✓ is otherwise involved in terrorism.
  - **Government can impose all-India bans on associations** which are declared 'unlawful' under the Act.
  - Both **Indian nationals and foreign nationals can be charged** under the Act. Also, Act holds offenders accountable in the same manner if **crime is committed on foreign land outside India.**
- **Investigating powers:** Cases can be **investigated by both State police and National Investigation Agency (NIA).**
- **Appeal mechanism:** It provides for **tribunal to review or to hear an appeal against** the ban.



Other Anti-terror laws

Terrorist and Disruptive Activities (Prevention) Act, 1987 - repealed in 2004

Prevention of Terrorism Act" (POTA), 2002 - repealed in 2004

Maharashtra Control of Organised Crime Act (MCOCA), 1999 - In force

Gujarat Control of Terrorism and Organised Crime (GCTOC) Act, 2019 - In force

### Significance of UAPA law in the contemporary times for India

- **To uproot terrorism from India:** Since 2001, 8,473 Indians have died at the hands of terrorists**.** Terrorists and insurgents continue to receive material support and funds.
- **Focus on individuals:** Not designating individuals as terrorists, would give them an opportunity to **circumvent the law and they would simply gather under a different name** and keep up their terror activities.
  - This is also important in the **context of lone wolf attacks, which do not belong to any organisation.**
- **Quickens process of justice delivery** by empowering officers in the rank of Inspector to investigate cases and investigation has to be completed within 90 days.
- **Reduces delay in attaching proceeds**: Act allows **seizure of property connected with terrorism** without taking approval of Director General of Police in case investigation is conducted by an officer of National Investigation Agency (NIA).

### Challenges of UAPA Act, 2019

- **Vague and unclear definitions:** Act does not define terrorism and definition of 'unlawful activity' is such that it covers almost every kind of violent act be it political or non-political.
- **Excessive discretionary powers:** No objective criterion has been laid for categorization of an individual as a terrorist and the government has been provided with "unfettered powers" to designate anyone as a terrorist.
- **Challenge to fundamental rights like Article 14, 19(1)(a), 21:** Act does not provide any opportunity to the individual termed as a terrorist to justify his case before the arrest. Those arrested under Act **can be imprisoned up to 180 days without a charge sheet being filed.**
- **Contrary to the principle of 'innocent until proven guilty:** Act violates mandate of Universal Declaration of Human Rights and International Covenant on Civil and Political Rights which recognize this principle as a **universal human right**.
- **Low conviction rate:** Only **2.2% of cases** registered under the UAPA between 2016 and 2019 resulted in conviction by courts.
- **Issue in the appeal process:** Act provides for appeal, but government itself will set up three-member review committee, two of whom can be serving bureaucrats.

### Conclusion

There is need for stringent laws to fight the terrorism so that authorities do not feel powerless while making a case against the accused but there is **need to balance human rights and constitutional values.**

The Act is crucial for expediting prosecution in terror cases. However, due process of law shall be followed by agencies involved under the Act at every stage. Also, the role of judiciary is paramount to keep a check on misuse of such laws.

## 3.2. FINANCIAL ACTION TASK FORCE

### Why in news?

Pakistan is likely to remain on the grey list of the **Financial Action Task Force (FATF)** for failing to comply with its deadline to prosecute and penalise terrorist financing in the country.

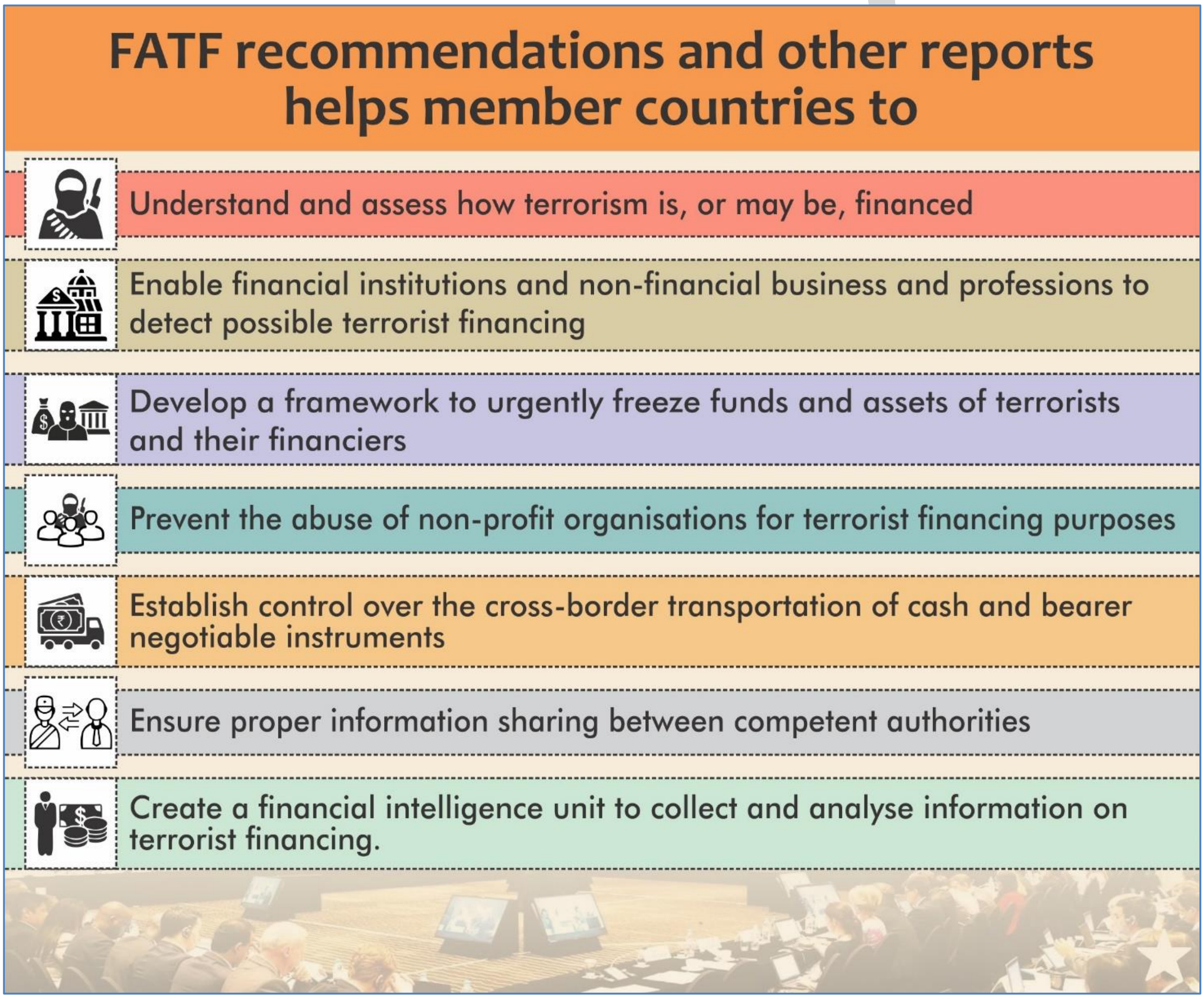
**About Financial Action Task Force (FATF)**

- The FATF is the **global money laundering and terrorist financing watchdog**.
- It **sets international standards** that aim to prevent these illegal activities and the harm they cause to society.
- It currently comprises **37 member countries (including India)** and 2 regional organizations-European Commission and Gulf Co-operation Council.
- It was established in July 1989 by a Group of Seven (G-7) Summit in Paris, **initially to examine and develop measures to combat money laundering.**
  - It **later expanded its mandate to incorporate efforts to combat terrorist financing** and to counter the financing of proliferation of weapons of mass destruction, in addition to money laundering.
- FATF established a series of **Special Recommendations to combat terrorism** which outlined measures to deprive terrorists and terrorist organisations of access to funding and the financial system.
  - Sources of terrorist financing vary from **legitimate funds** such as donations and money derived from charities to **unlawful funds** derived from activities such as drug trafficking, money laundering, smuggling, and illegal arms trading.

### Role of FATF in combating terrorist financing

- **Setting global standards to combat terrorist financing:** FATF ensures all its members have implemented measures to cut off terrorism-related financial flows, in accordance with the **FATF Recommendations.** All members are required to:
  - **Criminalise the financing** of individual terrorists and terrorist organisations.
  - **Freeze terrorist assets** without delay and implement ongoing prohibitions.
- **Evaluating countries' ability to prevent, detect, investigate and prosecute the financing of terrorism:** FATF issues two lists namely-
  - **Black list** (officially known as High-Risk Jurisdictions subject to a Call for Action)
    - ✓ It sets out the countries that are considered **deficient in their anti-money laundering and counter-financing of terrorism** (AML/CFT) regulatory regimes.

        - ✓ These blacklisted countries are **subjected to economic sanctions** and other prohibitive measures by FATF member states and other international organizations.
        - ✓ The current FATF blacklist includes two countries: **North Korea and Iran**.
    - **Grey list** (officially referred to as Jurisdictions Under Increased Monitoring)
        - ✓ Countries on the FATF grey list represent a much higher risk of money laundering and terrorism financing but have **formally committed to working with the FATF** to develop action plans that will address their AML/CFT deficiencies.
        - ✓ These countries are **subjected to increased monitoring** by the FATF.
        - ✓ While grey-list classification is not as negative as the blacklist, countries on the list may still face economic sanctions from institutions like the IMF and the World Bank and experience adverse effects on trade.
- **Assisting jurisdictions in implementing financial provisions of the United Nations Security Council resolutions on terrorism:** The FATF has developed a range of tools and guidance to help detect, disrupt, punish and prevent terrorist financing.



FATF recommendations and other reports helps member countries to

- Understand and assess how terrorism is, or may be, financed
- Enable financial institutions and non-financial business and professions to detect possible terrorist financing
- Develop a framework to urgently freeze funds and assets of terrorists and their financiers
- Prevent the abuse of non-profit organisations for terrorist financing purposes
- Establish control over the cross-border transportation of cash and bearer negotiable instruments
- Ensure proper information sharing between competent authorities
- Create a financial intelligence unit to collect and analyse information on terrorist financing.

## 3.3. BIO-TERRORISM

**Why in news?**

Parliamentary panel has **highlighted the need for the government to have laws to counter bio-terrorism** in its report 'The Outbreak of Pandemic COVID-19 and its Management'.

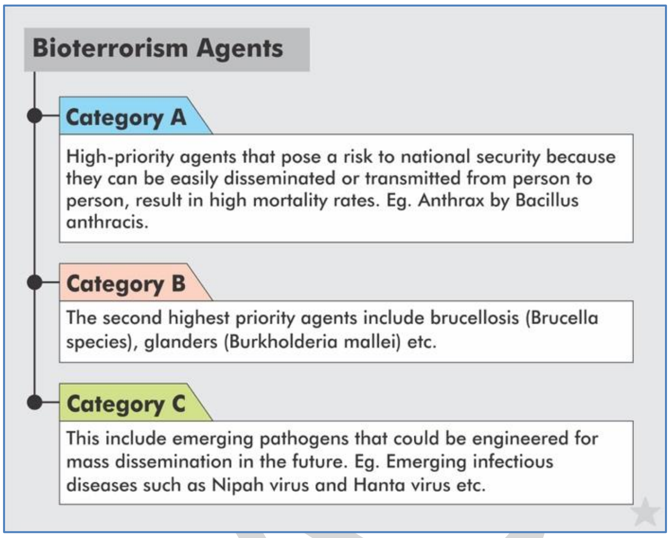
**About bio-terrorism**

- **Bioterrorism is a planned and deliberate use of pathogenic strains of microorganisms** such as bacteria, viruses, or their toxins to spread life-threatening diseases on a mass scale in order to devastate the population of an area.

- These agents are **delivered by Scud missiles, motor vehicles with spray, hand pump sprayers, book or letter, guns, remote control, robots** etc.
- It is often difficult to monitor the origin of such diseases/attacks.

**Need for Bio terrorism law in India**

- **India's high vulnerability**: High population density, Inadequate medical facilities, subtropical climatic conditions, poor hygiene and inadequate sanitation facilities make India extremely susceptible for such attacks.
- **Control its impact on society**: Bioterrorism causes damage, fear, and anxiety among people and affects the society and government of a country. These biologic weapons can cause large-scale mortality and morbidity in large population and create civil disruption in the shortest possible time.
- **Increase in attacks due to advancement in technology:** The present era of biotechnology and nanotechnology has created an easy accessibility to more sophisticated biologic agents apart from the conventional bacteria, viruses and toxins.



Bioterrorism Agents

Category A

High-priority agents that pose a risk to national security because they can be easily disseminated or transmitted from person to person, result in high mortality rates. Eg. Anthrax by Bacillus anthracis.

Category B

The second highest priority agents include brucellosis (Brucella species), glanders (Burkholderia mallei) etc.

Category C

This include emerging pathogens that could be engineered for mass dissemination in the future. Eg. Emerging infectious diseases such as Nipah virus and Hanta virus etc.

**Mechanism to counter bio-terrorism**

- **Deterrence by law:** There is a need to introduce Public Health Bill on the line of **Public Health (Prevention, Control and Management of epidemics, bio-terrorism and disasters) Bill-2017**, which defined terms epidemic, isolation, quarantine and social distancing, but lapsed.
    - Bill also **needs to repeal Epidemic Diseases Act of 1897,** which is not specific to biological threat and does not define terms.
- **Prevention**: This is to be done through examining the risk of bioterror attacks, case studies, prevention of attacks, preparation and training of law enforcement personnel, and the related legal and political framework for enhanced intelligence.
- **Surveillance and assessment**: This can be done by recognizing patterns of non-specific syndromes and assessing them, that could indicate the early manifestations of a biological warfare attack.
- **Laboratory investigation:** Primary healthcare providers, laboratory staff, are the first responders and will most likely identify the initial cases.
    - Hence **in conjunction with infection control and administrative personnel should develop both laboratory- and institution-wide response plans** for diagnosis and characterization of the biological organism.

**Existing measures to counter bio-terrorism in India**

- **Epidemic Diseases Act of 1897** to provide for the better prevention of the spread of Dangerous Epidemic Diseases by providing special powers to authorities.
- **National Disaster Management Authority (NDMA):** NDMA has proposed a model instrument where participation of both government and private sectors is a pre-requisite to manage the menace of biological disaster.
- **Integrated Disease Surveillance Project (IDSP):** It was initiated in assistance with World bank, to strengthen/maintain decentralized laboratory-based IT enabled disease surveillance system for epidemic-prone diseases to monitor disease trends and to detect and respond to outbreaks in early rising phase through trained Rapid Response Team.
- **International Health Regulations:** Revised International Health Regulations came into force in India in June 2007, that helps to ensure that outbreaks and other public health emergencies of international concern are detected and investigated more rapidly.

**Initiatives at international level**

- **Biological Weapons Convention:** It is first multilateral disarmament treaty banning the development, production and stockpiling of Bacteriological (Biological) and Toxin Weapons.
- **INTERPOL Bioterrorism Prevention Unit:** It aims to enable law enforcement agencies to prevent, prepare and respond to the deliberate use of bacteria, viruses or biological toxins that threaten or cause harm to humans, animals or agriculture.
- **Cartagena Protocol on Biosafety:** It is an international agreement which aims to ensure the safe handling, transport and use of living modified organisms (LMOs) resulting from modern biotechnology.

- **Medical management:** It should include preventive, promotive, and curative services like Chemoprevention to prevent the spread of the disease.
- **General public sensitization:** This can be done by law enforcing agencies, through training and education, warning network at hospitals and public health agencies etc.

## 3.4. NAXAL VIOLENCE

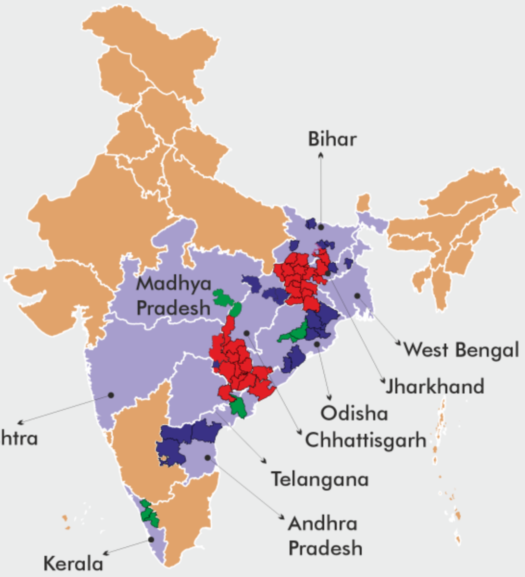
**Why in news?**

In an encounter between central paramilitary forces and Maoists in Chhattisgarh's Sukma, 22 personnel died.

**Naxalism in India**

- Naxalism is a form of **armed insurgency against the State** motivated by leftist/maoist ideologies and thus is **also known as Left Wing extremism (LWE) or Maoism**.
- The Naxal insurgency in India **originated in a 1967 uprising in Naxalbari, West Bengal** by the Communist Party of India (Marxist).
  - They are the group of people who believe in the political theory derived from the teachings of the Chinese political leader **Mao Zedong**.
- The Naxalites claim to represent the most oppressed people in India, those who are often left untouched by India's development and bypassed by the electoral process.
- The conflict is **concentrated in the Eastern part of the country**, particularly an area known as the **Red Corridor** spread across the states of Chhattisgarh, Odisha, Jharkhand, Bihar and Andhra Pradesh.
- **Counterinsurgency operation by the Centre and affected states** have helped to bring down Maoist sponsored violence. **Covid-19 pandemic and the national lockdown** also proved a massive blow for Maoists, as it cut critical supplies for many months.
- As a result, **LWE related incidents were down by 47 per cent** between 2015 and 2020 as compared to incidents in the preceding six years from 2009 to 2014.

**Areas affected by Naxal violence**



**SHRINKING RED CORRIDOR**

What a recent MHA survey has said about Left Wing Extremism-affected districts

🟩 **DISTRICTS ADDED TO LWE-AFFECTED LIST**

**CHHATTISGARH**: Kabirdham
**KERALA**: Wayanad,Malappuram, Palakkad
**MADHYA PRADESH:** Mandla
**ODISHA**: Boudh,Angul
**ANDHRA PRADESH**: West Godavari

🟦 **SOME DISTRICTS REMOVED FROM LWE-AFFECTED LIST**

**ODISHA**: Keonjhar, Mayurbhanj, Ganjam, Gajapati, Dhenkanal, Jaipur
**BIHAR**: Patna, Bhojpur, Sheohar, Sitamarhi, Begusarai, Khagaria
**CHHATTISGARH**: Sarguja, Korea, Jashpur
**ANDHRA PRADESH**: Prakasam, Kurnool, Anantapur
**JHARKHAND**: Deogarh, Pakur
**MAHARASHTRA**: Aheri

🟥 **THIRTY MOST-AFFECTED LWE DISTRICTS**

**CHHATTISGARH**: Sukma, Rajnandgaon, Narayanpur, Kondagaon, Kanker, Dantewada, Bijapur, Bastar
**JHARKHAND**: Bokaro, Chatra, Garhwa, Giridih, Gumla, Hazaribagh, Khunti, Latehar, Lohardaga, Palamu, Simdega West, Ranchi, Singhbhum
**ODISHA** : Koraput, Malkangiri
**TELANGANA**: Bhadradri
**BIHAR** : Lakhisarai, Jamui, Gaya, Aurangabad
**ANDHRA PRADESH**: Visakhapatnam
**MAHARASHTRA**: Gadchiroli

- Presently, 90 districts in 11 states in the country are considered LWE affected.
- **Chhattisgarh and Jharkhand continue to account for 69.10% incidents** of naxal violence across the country.

### Causes for Spread of Left Extremism

| | |
|---|---|
| **Land Related Factors** | • Evasion of land ceiling laws.<br>• Existence of special land tenures (enjoying exemptions under ceiling laws).<br>• Encroachment and occupation of Government and Community lands (even the water-bodies) by powerful sections of society.<br>• Lack of title to public land cultivated by the landless poor.<br>• Poor implementation of laws prohibiting transfer of tribal land to non-tribals in the Fifth Schedule areas<br>• Non-regularisation of traditional land rights. |
| **Governance Related Factors** | • Corruption and poor provision/non-provision of essential public services including primary health care and education.<br>• Incompetent, ill-trained and poorly motivated public personnel<br>• Misuse of powers by the police and violations of the norms of law.<br>• Perversion of electoral politics and unsatisfactory working of local government institutions.<br>• In 2006, Forest Rights Act was enacted. But Forest Bureaucracy continued its hostility towards it. |
| **Displacement and Forced Evictions** | • Eviction from lands traditionally used by tribals.<br>• Displacements caused by mining, irrigation and power projects without adequate arrangements for rehabilitation.<br>• Large scale land acquisition for 'public purposes' without appropriate compensation or rehabilitation. |
| **Livelihood Related Causes** | • Lack of food security<br>• Disruption of traditional occupations and lack of alternative work opportunities.<br>• Deprivation of traditional rights in common property resources. |

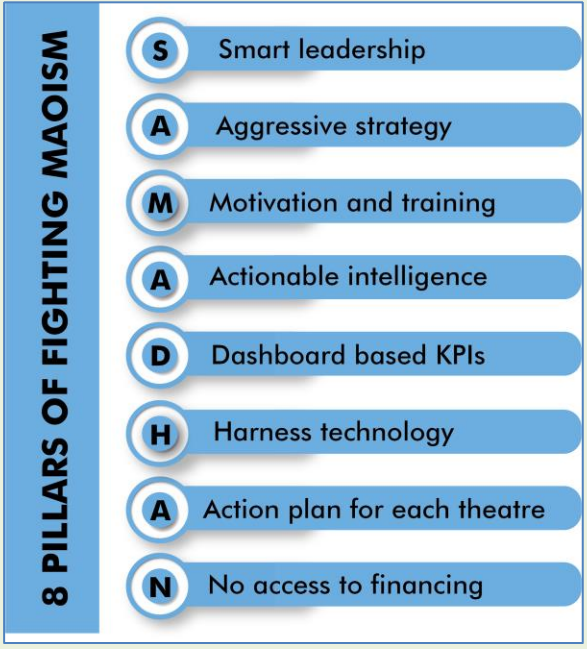
### Important Initiatives for LWE affected states

'Police' and 'Public order' being State subjects, the primary responsibility of meeting the challenge of Left Wing Extremism (LWE) lies with the State Governments. However, the MHA and other central ministries supplement the security efforts of the State Governments through various schemes such as:

- **National Policy and Action Plan** implemented by MHA since 2015 is a multi-pronged strategy in the areas of security, development, ensuring rights & entitlement of local communities etc. to combat LWE.
- **Major Sub –Schemes under Scheme Modernization of Police Forces for 2017-21**
  - **Security Related Expenditure (SRE) Scheme** (approved in 2017): aims at strengthening the capacity of the LWE affected States to fight against the LWE problem in an effective manner.
  - **Special Central Assistance** (SCA) for 30 most LWE affected districts to fill the critical gaps in Public infrastructure and Services,
  - **Special Infrastructure Scheme** (SIS) including construction of 250 Fortified Police Stations in LWE affected states.
  - **Assistance to Central Agencies for LWE management Scheme**
  - **Civic Action Programme** (CAP) to bridge the gaps between Security Forces and local people through personal interaction.
  - **Media Plan Scheme** to counter the Maoist propaganda.
- **Infrastructure development initiatives**
  - **Road Requirement Plan-I and II (RRP-I&II)** is being implemented by Ministry of Road Transport & Highways, for improving road connectivity in affected districts.

**SAMADHAN**

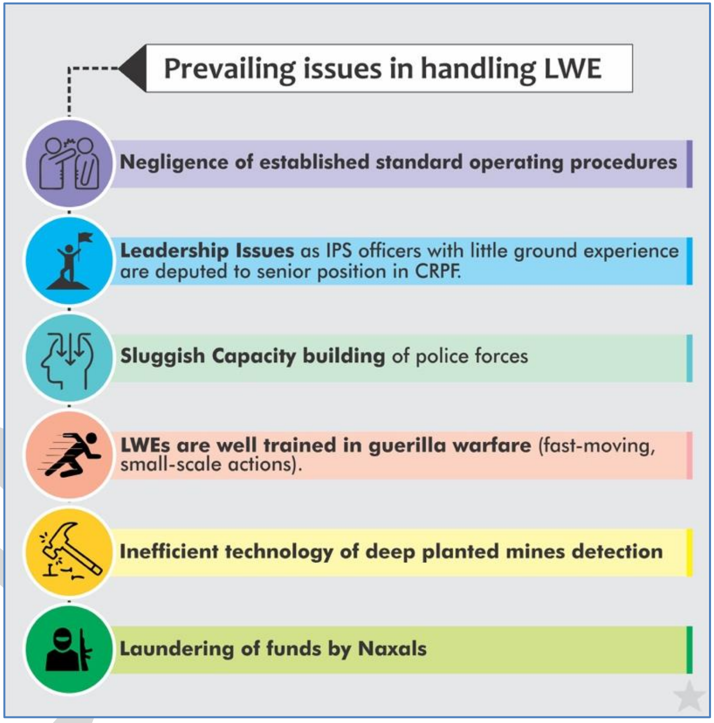
It is a strategy of MHA to frame short term and long-term policies to tackle LWE. It includes:



8 PILLARS OF FIGHTING MAOISM

- S Smart leadership
- A Aggressive strategy
- M Motivation and training
- A Actionable intelligence
- D Dashboard based KPIs
- H Harness technology
- A Action plan for each theatre
- N No access to financing

- LWE Mobile Tower Project and approval of Projects under Universal Service Obligation Fund (USOF) to improve mobile connectivity.
  - **The National Technical Research Organization** (NTRO) is assisting the Security Forces in anti-Naxal operations by providing Unmanned Aerial Vehicles (UAVs).
- **Skill Development related Schemes**
  - **ROSHNI** is a special initiative under, Pandit Deen Dayal Upadhyaya Grameen Kaushalya Yojana which envisages training and placement of rural poor youth from affected districts.
  - **ITIs and Skill Development Centres** have been established in LWE affected districts.
- **Institutional measures**
  - **Black Panther combat force** - A specialised anti-Naxal combat force for Chhattisgarh on the lines of Greyhounds unit in Telangana and Andhra Pradesh.
  - **Bastariya Batallion** – A newly formed batallion of CRPF with tribal youth from four highly naxal infested districts of Chhattisgarh along with adequate female representation.


Prevailing issues in handling LWE

**Negligence of established standard operating procedures**

**Leadership Issues** as IPS officers with little ground experience are deputed to senior position in CRPF.

**Sluggish Capacity building** of police forces

**LWEs are well trained in guerilla warfare** (fast-moving, small-scale actions).

**Inefficient technology of deep planted mines detection**

**Laundering of funds by Naxals**

  - **Separate vertical in the NIA** has been created for investigating cases.
  - **Multi-disciplinary groups to check funding of Naxalites** - MHA has formed multi-disciplinary groups with officers from central agencies, including from the IB, NIA, CBI, ED and DRI, and state police to choke the financial flow to Maoists.
- **Constructively engaging youth through education:** Seeing the success of educational hub and a livelihood centre in Dantewada district, the government has now opened up livelihood centres, known as **Livelihood Colleges**, in all the districts.
- **Other measures:**
  - **More bank branches** have been opened to ensure financial inclusion.
  - **All India Radio stations** in Bastar broadcast regional programmes to increase entertainment options.

**Success story: Grey Hounds in Andhra Pradesh**

- In 1989, Andhra Pradesh set up Greyhounds, **an elite force trained in jungle warfare** and counter-Maoist strategy that carried out pin-pointed operations with great success.
- This was **coupled with a surrender-and-rehabilitation policy** and setting up of the Remote and Interior Area Development Department to ensure that welfare schemes and infrastructure projects were tailored for Maoist areas.
- Nearly 10 years after the formation of the Greyhounds, by 1999, the state police started getting an upper hand. With the occasional setbacks, by 2011, Andhra Pradesh finally managed to eliminate the Maoists.

## Way forward

The two-pronged policy of proactive policing and holistic development is showing results and must be continued for significant results in the future. This includes:

- **Learning from best practices: Grey hounds in Andhra Pradesh** have been successful in minimising Maoists activities to a large extent. Similarly, as **Chhattisgarh police** have experience in tackling Maoists in Bastar, they are now coordinating with the bordering States to strengthen intelligence and ground presence.
- **Eliminating the root cause of the problem** that is leading to the alienation of tribals in this area. The focus should now be on:
  - **Financial empowerment:** Introduce measures to encourage formation of 'Self Help Groups' (SHGs) to improve access to credit and marketing and empower the disadvantaged.
  - **Infrastructure development:** For implementing large infrastructure projects, particularly road networks that are strongly opposed by the extremists can be undertaken with the help of specialised Government agencies like the Border Roads Organisation instead of local contractors.
  - **Forest Rights:** Effective implementation of the Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Rights) Act, 2006.

- **Cooperative federalism**: Centre and states should continue with their coordinated efforts where Centre should play a supportive role with state police forces taking the lead.
- **Leveraging the use of technology:** Such as micro or mini-UAVs or small drones, high-resolution PTZ cameras, GPS tracking, hand-held thermal imaging, radar and satellite imaging to minimize loss of lives of security personnel. Also, technologies like trackers in weapons and biometrics in smart guns must be used, to check the use of looted arms by the militants.
- **Choke funding:** The nexus between illegal mining/forest contractors and transporters and extremists which provides the financial support for the extremist movement needs to be broken through establishment of special anti-extortion and anti-money laundering cell by State Police.
- **Role of the media in building trust and awareness generation:** Support of media must be taken in order to change the sympathetic attitude of people towards the Maoists, to dispel the fear created by the Naxalites in the minds of people and instil confidence among them that the State is by their side.

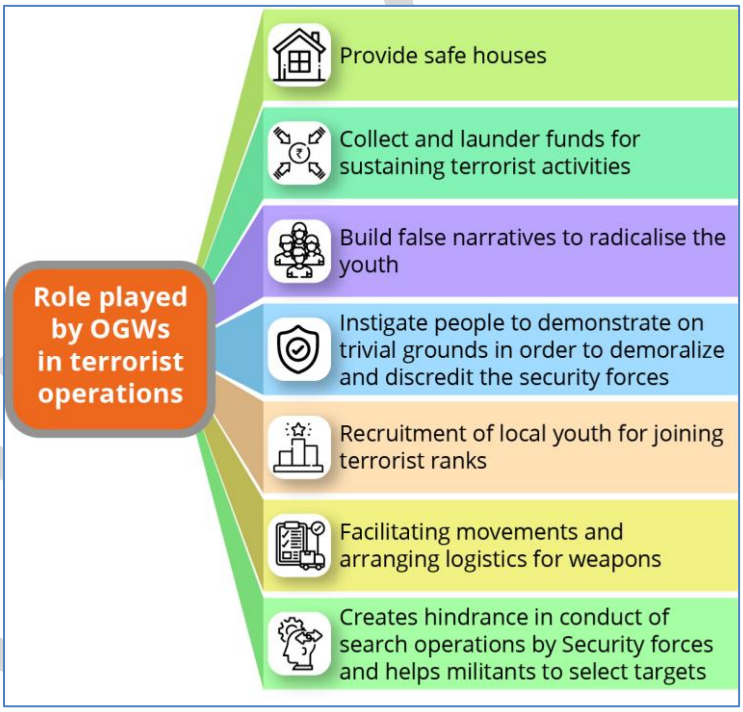
## 3.5. OVERGROUND WORKERS (OGWS)

**Why in News?**

Jammu and Kashmir (J&K) police recently arrested three overground workers (OGWs) for a grenade attack on a Central Reserve Police Forces (CRPF) camp.

**Who are overground workers?**

- The Jammu and Kashmir Police categorize **"anybody who supports the militants" as an OGW**.
  - A person **providing a safe house, passage, information or acting as a messenger** for suspected militants automatically is categorized as an OGW.
- OGWs are often described as **'militants without weapons'**.
- They are generally recruited by employing a strategy of **systematic entrapment** which starts out with radicalization of youth, which progresses into more serious crimes and culminates into being an OGW.



Role played by OGWs in terrorist operations

Provide safe houses

Collect and launder funds for sustaining terrorist activities

Build false narratives to radicalise the youth

Instigate people to demonstrate on trivial grounds in order to demoralize and discredit the security forces

Recruitment of local youth for joining terrorist ranks

Facilitating movements and arranging logistics for weapons

Creates hindrance in conduct of search operations by Security forces and helps militants to select targets

- OGWs have the potential to become future militants.
  - Terror groups like Hizb-ul-Mujahideen and Lashker-e-Toiba have a well-established network of OGWs which is sustaining militancy in Kashmir.

**Issues in handling OGWs**

- **Extreme steps can increase militancy**: Random booking of youth for suspected OGW activity can completely eliminates an individual's chance to come back to society and thus provide opportunity to the terrorists for indoctrination.
- **Negative perception of Government**: Government's operations towards OGWs can embed strong 'Us vs Them' narratives amongst the population and alienate them from the Indian polity.
- **Harder to track:** OGWs are also capable of carrying out small scale strikes while retaining the capability to mix rapidly with the population.

**Measures to tackle OGWs**

- **Need to jointly map the OGWs, terrorists and anti-national elements through a multi-agency effort** so that the intelligence picture generated is in sync with ground realities.
- **Youth engagement programmes** should be widened to include addressing their sense of alienation and the trust deficit.
  - For instance, Youth forums can be conducted as platforms where political, social and cultural issues can be freely discussed.
- **Evolve a long-term de-radicalization and counter-radicalization policy for Kashmir**: This would require detailed exploration by subject-experts, but it must be multidisciplinary in its approach, roping in religious

scholars, experts in the philosophy of religion and politics, experts in cyber-jihad, psychologists, educationists, civil society members, etc.

- **Psychological and social rehabilitation as well as strategic communication** can change their mind set and bring them back into the mainstream.
- **Launching intelligence-based sting operations** over a period of time to gather proof of their damaging activities and exposing them.
- **Investing in artificial intelligence (AI) and other technologies** to discourage extremist content on social media.

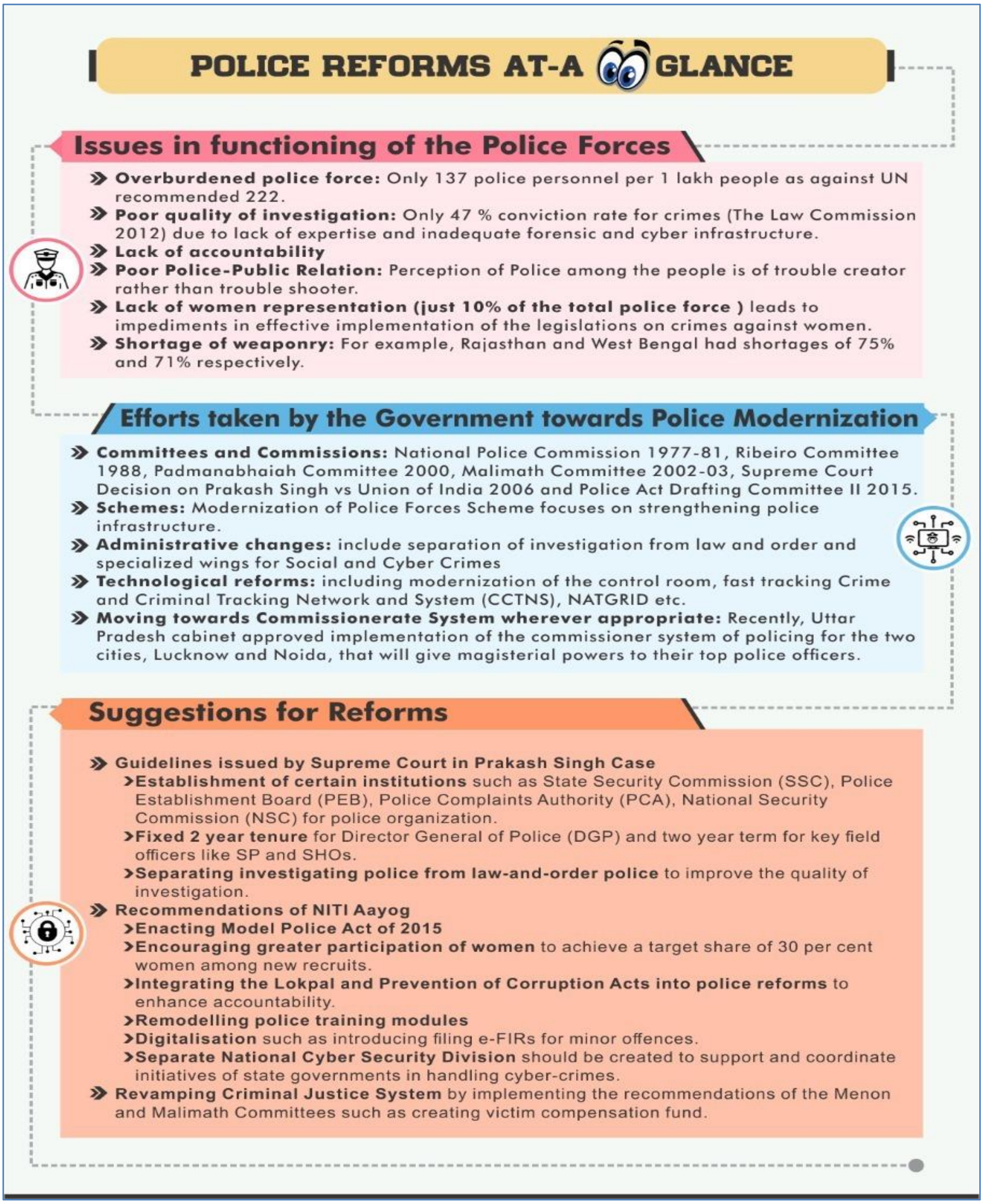
**Steps taken in India to deal with OGWs**

- **Operation All Out** was launched in 2017 by the Indian armed forces to eliminate the militant networks, their OGW, and top militant commanders.
- **Jammu and Kashmir Public Safety Act, 1978 (PSA)** is used to book anti national elements and OGWs to prevent them from disrupting peace and security.
- **Operation Sadbhavana (Goodwill)** is a unique humane initiative undertaken by Indian Army in Jammu & Kashmir to address aspirations of people affected by terrorism with focus on improving the overall core social indices of Education, Women & Youth Empowerment, and Health care with simultaneous thrust on capacity building through implementation of community/infrastructure development projects.
- **Mission Pehal** launched in 2021: Under it, officers conduct face-to-face interactions with the Kashmiri youth to encourage the youth to express their grievances and the reasons they may have for mistrusting the Indian state; the Army officers.
- **Education scholarships and livelihood schemes** such as USTTAD, Udaan, and Nai Manzil.
- **Training and employment opportunities for the youth of Jammu and Kashmir** are also provided under many schemes such as HIMAYAT and **Pradhan Mantri Kaushal Vikas Yojana** (**PMKVY**).
- **Utilization of the social media platforms** by the armed forces, alongside the local police, for limiting extremist content and narratives on social media by monitoring and reporting them to tech platforms, and countering them with genuine news.
- **Other steps by Law enforcing agencies include**-
  - enhanced interaction between police and public at various levels.
  - sharing of intelligence inputs on real time basis amongst all security forces operating in Jammu and Kashmir.
  - intensified area domination of militancy affected areas by deployment of additional Nakas and patrolling by security forces etc.
  - Tracking flow of funds to terrorist organisations by National Investigative Agency (NIA).

# 4. POLICE REFORMS

**Overview**

Police organization is based on the Police Act of 1861. Since then, the issues faced by the Police Organization have evolved in complexity with changing nature of crimes. Thus, the demand for better efficacy and more democratization of the police force has paved the way for progressive modernization of the Police as an institution.



## POLICE REFORMS AT-A GLANCE

### Issues in functioning of the Police Forces

- **Overburdened police force:** Only 137 police personnel per 1 lakh people as against UN recommended 222.
- **Poor quality of investigation:** Only 47 % conviction rate for crimes (The Law Commission 2012) due to lack of expertise and inadequate forensic and cyber infrastructure.
- **Lack of accountability**
- **Poor Police-Public Relation:** Perception of Police among the people is of trouble creator rather than trouble shooter.
- **Lack of women representation (just 10% of the total police force )** leads to impediments in effective implementation of the legislations on crimes against women.
- **Shortage of weaponry:** For example, Rajasthan and West Bengal had shortages of 75% and 71% respectively.

### Efforts taken by the Government towards Police Modernization

- **Committees and Commissions:** National Police Commission 1977-81, Ribeiro Committee 1988, Padmanabhaiah Committee 2000, Malimath Committee 2002-03, Supreme Court Decision on Prakash Singh vs Union of India 2006 and Police Act Drafting Committee II 2015.
- **Schemes:** Modernization of Police Forces Scheme focuses on strengthening police infrastructure.
- **Administrative changes:** include separation of investigation from law and order and specialized wings for Social and Cyber Crimes
- **Technological reforms:** including modernization of the control room, fast tracking Crime and Criminal Tracking Network and System (CCTNS), NATGRID etc.
- **Moving towards Commissionerate System wherever appropriate:** Recently, Uttar Pradesh cabinet approved implementation of the commissioner system of policing for the two cities, Lucknow and Noida, that will give magisterial powers to their top police officers.

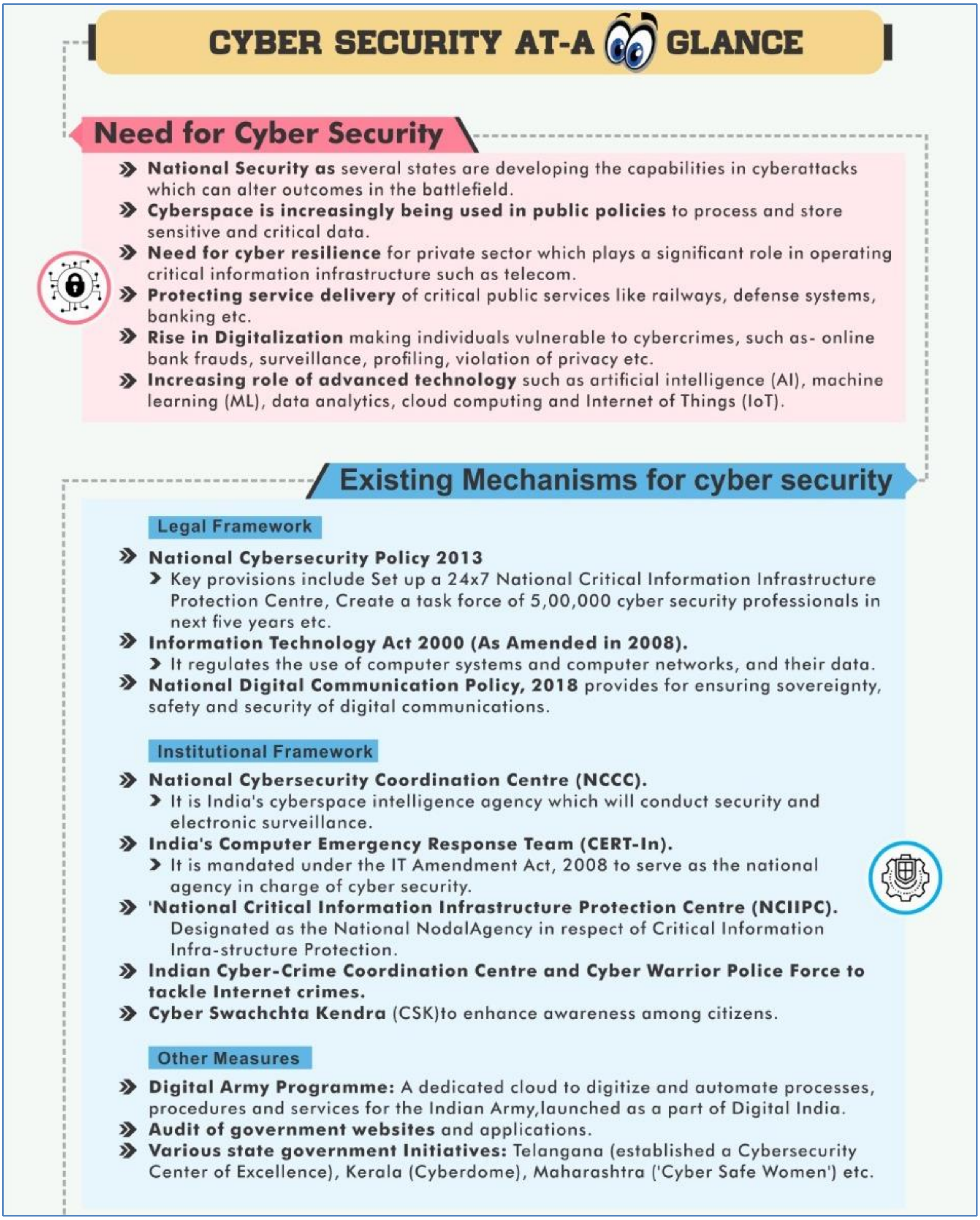
### Suggestions for Reforms

- **Guidelines issued by Supreme Court in Prakash Singh Case**
  - **Establishment of certain institutions** such as State Security Commission (SSC), Police Establishment Board (PEB), Police Complaints Authority (PCA), National Security Commission (NSC) for police organization.
  - **Fixed 2 year tenure** for Director General of Police (DGP) and two year term for key field officers like SP and SHOs.
  - **Separating investigating police from law-and-order police** to improve the quality of investigation.
- **Recommendations of NITI Aayog**
  - **Enacting Model Police Act of 2015**
  - **Encouraging greater participation of women** to achieve a target share of 30 per cent women among new recruits.
  - **Integrating the Lokpal and Prevention of Corruption Acts into police reforms** to enhance accountability.
  - **Remodelling police training modules**
  - **Digitalisation** such as introducing filing e-FIRs for minor offences.
  - **Separate National Cyber Security Division** should be created to support and coordinate initiatives of state governments in handling cyber-crimes.
- **Revamping Criminal Justice System** by implementing the recommendations of the Menon and Malimath Committees such as creating victim compensation fund.

# 5. CYBERSECURITY

**Overview**

- Cyber Security is the process of **securing information or assets that are contained in cyberspace** from unauthorised access, use, disclosure, disruption, modification or destruction.
    - Cyberspace comprises interaction between people, software and services, supported by worldwide distribution of information and communication technology devices and networks.
- **India is ranked 10th (among 194 countries)** in the Global Cybersecurity index (GCI) 2020 ahead of China and Pakistan.



CYBER SECURITY AT-A GLANCE

## Need for Cyber Security

- **National Security as** several states are developing the capabilities in cyberattacks which can alter outcomes in the battlefield.
- **Cyberspace is increasingly being used in public policies** to process and store sensitive and critical data.
- **Need for cyber resilience** for private sector which plays a significant role in operating critical information infrastructure such as telecom.
- **Protecting service delivery** of critical public services like railways, defense systems, banking etc.
- **Rise in Digitalization** making individuals vulnerable to cybercrimes, such as- online bank frauds, surveillance, profiling, violation of privacy etc.
- **Increasing role of advanced technology** such as artificial intelligence (AI), machine learning (ML), data analytics, cloud computing and Internet of Things (IoT).

## Existing Mechanisms for cyber security

**Legal Framework**

- **National Cybersecurity Policy 2013**
    - Key provisions include Set up a 24x7 National Critical Information Infrastructure Protection Centre, Create a task force of 5,00,000 cyber security professionals in next five years etc.
- **Information Technology Act 2000 (As Amended in 2008).**
    - It regulates the use of computer systems and computer networks, and their data.
- **National Digital Communication Policy, 2018** provides for ensuring sovereignty, safety and security of digital communications.

**Institutional Framework**

- **National Cybersecurity Coordination Centre (NCCC).**
    - It is India's cyberspace intelligence agency which will conduct security and electronic surveillance.
- **India's Computer Emergency Response Team (CERT-In).**
    - It is mandated under the IT Amendment Act, 2008 to serve as the national agency in charge of cyber security.
- **'National Critical Information Infrastructure Protection Centre (NCIIPC).** Designated as the National NodalAgency in respect of Critical Information Infra-structure Protection.
- **Indian Cyber-Crime Coordination Centre and Cyber Warrior Police Force to tackle Internet crimes.**
- **Cyber Swachchta Kendra** (CSK)to enhance awareness among citizens.

**Other Measures**

- **Digital Army Programme:** A dedicated cloud to digitize and automate processes, procedures and services for the Indian Army,launched as a part of Digital India.
- **Audit of government websites** and applications.
- **Various state government Initiatives:** Telangana (established a Cybersecurity Center of Excellence), Kerala (Cyberdome), Maharashtra ('Cyber Safe Women') etc.

## Challenges to Cyber Security in India

**Structural**

- **Absence of any geographical constraints.**
- **Lack of uniformity in devices used for internet access.**

**Administrative**

- **Lack of national level architecture for Cybersecurity.**
- **Security audit does not occur periodically,** nor does it adhere to the international standards.
- The appointment of National Cyber Security Coordinator in 2014 has not been supplemented by the creating liaison officers in states.

**Procedural**

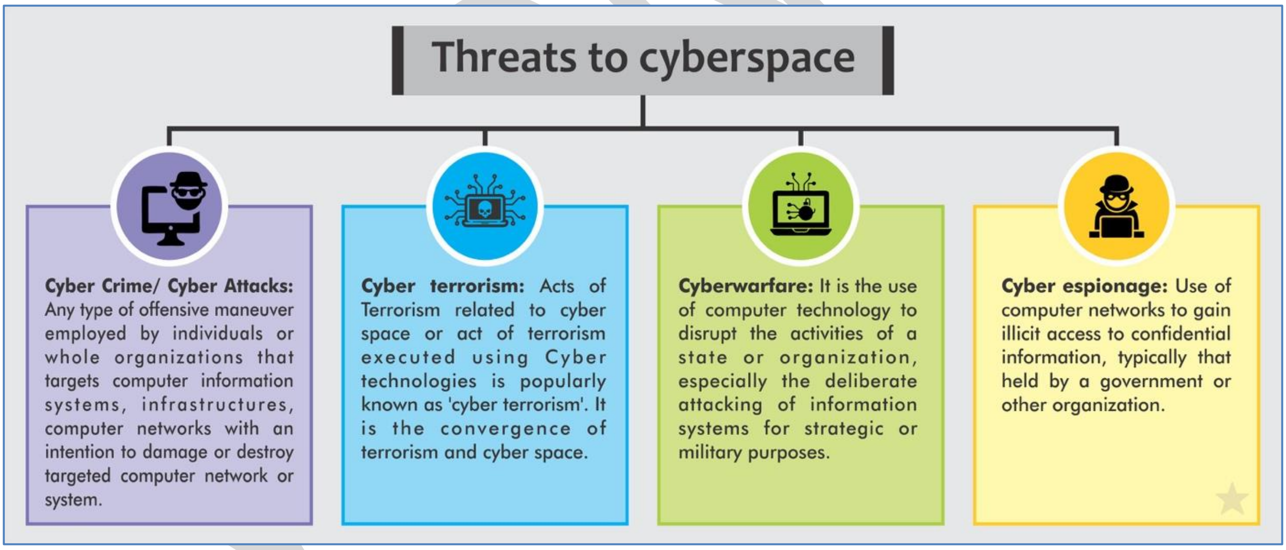
- **Lack of awareness in local police of various** provisions of IT Act, 2000 and also of IPC related to cybercrimes.
- **Lack of data protection regime.**

**Human Resource Related**

- **Inadequate awareness among people** about security of devices and online transactions.

## Way Forward

- **Information sharing and coordination** among agencies like DRDO, NTRO, CERT-In, RAW, IB etc.
- **PPP Model for Cybersecurity** to ensure protection of private sector Critical Information Infrastructure
- **Capacity building and skill development.**
- **Promoting startups** in the field of digital security.
- **Learning from best practices** such as Tallinn Manual of US.



Threats to cyberspace

**Cyber Crime/ Cyber Attacks:** Any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks with an intention to damage or destroy targeted computer network or system.

**Cyber terrorism:** Acts of Terrorism related to cyber space or act of terrorism executed using Cyber technologies is popularly known as 'cyber terrorism'. It is the convergence of terrorism and cyber space.

**Cyberwarfare:** It is the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.

**Cyber espionage:** Use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization.

## 5.1. CRITICAL INFRASTRUCTURE

**Why in News?**

After a suspected cyber-attack on Mumbai power grid by Chinese hackers, Government has recently released guidelines for the **Cyber Security in Power Sector**.

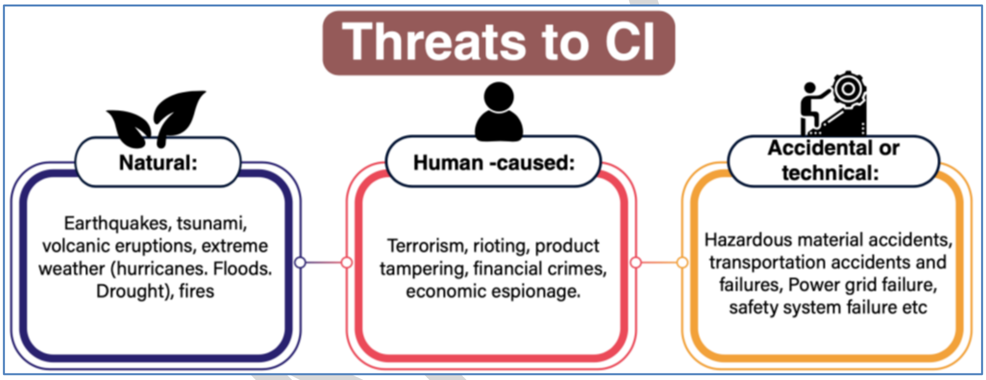
**More about the guidelines**

- The guidelines have been **framed by the Central Electricity Authority under the provision of Section 3(10)** on Cyber Security in the 'Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019'
- These are **applicable to all Responsible Entities** including power generation utilities, distribution utilities etc**. engaged in the Indian power supply system.**

- **Objective:** To ramp up security measures across various utilities to raise preparedness in power sector.
- **Major guidelines are:**
    - **Procurement from Trusted Source:** ICT based procurement should be from identified 'Trusted Sources' and identified 'Trusted Products' or else the product has to be tested for Malware/Hardware Trojan before deployment for use in power supply system network.
    - **Appointment of a Chief Information Security Officer (CISO)** at each responsible entity as well as the setting up of an Information Security Division headed by the CISO.
    - **Identifying and Reporting threats:** The entities will be required to incorporate a procedure for identifying and reporting any disturbances suspected or confirmed to be caused by sabotage and submit the report to the sectoral CERT and Computer Emergency Response Team -India (CERT-In) within 24 hours.

### About Critical Infrastructure

- Critical infrastructure (CI) refers to those **essential physical and information technology facilities**, networks, services and assets, which, if disrupted or destroyed, would have a serious impact on the health, safety, security, economic or social well-being or the effective functioning of government.
    - **Chemicals, Dams, emergency services, Power & Energy, Banking & financial services,** government facilities, healthcare, information technology, transportation, nuclear reactors etc. are considered parts of CI of a country.



Threats to CI

**Natural:** Earthquakes, tsunami, volcanic eruptions, extreme weather (hurricanes. Floods. Drought), fires

**Human -caused:** Terrorism, rioting, product tampering, financial crimes, economic espionage.

**Accidental or technical:** Hazardous material accidents, transportation accidents and failures, Power grid failure, safety system failure etc

### Importance of Critical infrastructure security

- **Vital for economic prosperity:** Resilient and secure infrastructure not only underpins the effective operating of businesses and services, but also long term confidence and planning in a region, and thus ongoing investment levels.
- **Cascading effects:** Loss, damage, unavailability, though for a short duration, can have significant consequences far beyond the targeted sector and physical location of the incident.
- Disruptions to CI could **impact global supply chain.**

### Challenges in protecting critical infrastructure

- **Internal Resources:** Many organizations including those that help to maintain Critical Infrastructure do not have enough **trained security professionals** to meet their security needs.
- **Reluctance in Sharing Information:** Fear of losing a competitive edge over rivals inhibits the private and public sector to share information about the vulnerability of their systems.
- **Lack of co-ordination among agencies:** Some of the agencies report to the Ministry of Home Affairs, while others report to the Prime Minister's Office, Defence ministry, MeitY etc.
- **Capability Asymmetry:** India lacks indigenization in hardware as well as software cybersecurity tools. This makes India's cyberspace vulnerable to cyberattacks motivated by state and non-state actors.

### Way forward

- **Need to evolve a comprehensive security policy** to address the physical, legal, cyber and human dimensions of security.
- **A better understanding of vulnerabilities is required**, including interdependencies between infrastructures.
- A functioning **partnership between the state and the corporate sector is essential.**
- An **integrated and sustainable supply chain security objective** must be included in business plans, contracts and operations.

## 5.1.1. NATIONAL SECURITY DIRECTIVE ON THE TELECOM SECTOR

**Why in news?**

Considering the need to ensure India's national security, the Cabinet Committee on Security has accorded approval for the **National Security Directive on the Telecom Sector**.

**Background**

- Indian directives for telecom security come **amid global security concerns raised against Chinese equipment maker Huawei**.
- **India has restricted investments from Huawei** for the rollout of 5G networks, which was also banned by UK and US government for on ground of national security.
- **India has also banned** over 200 Chinese mobile apps under Section 69A of the Information Technology Act.

**About telecom industry in India**

- Currently, India is the **world's second-largest telecommunications market** with a subscriber base of 1.16 billion and tele-density of 87.37% in FY20.
- India also ranks as the **world's second largest market in terms of total internet users** with subscribers at 743.19 million in FY20.
- It is expected that over the **next five years, rise in mobile-phone penetration and decline in data costs will add 500 million new internet users** in India, creating opportunities for new businesses.

**About National Security Directive on the Telecom Sector**

NSDTS is **India's first and biggest framework to protect itself from cyber-attacks,** data theft and other virtual vulnerabilities threatening its national security. Under it,

- **National Security Committee on Telecom (NSCT) headed by the deputy National Security Advisor** will identify trusted sources of telecom equipment that can be used by India's cellular operators on their networks.
    - It will also **release the names of the firms** whose equipment cannot be used.
- To qualify as domestic players in the trusted category, they should meet **the criteria of the Department of Telecommunications' preferential market access (PMA) scheme.**
    - **PMA scheme** is for providing preference to domestically manufactured electronic products, in procurement of those electronic products which have security implications for the country.
- **New devices have to mandatorily be procured from trusted sources.**
- **Department of Telecom will make appropriate modifications in the licence conditions** for the implementations of the provisions of the directive.

**Why there is need to have telecom security?**

Rising telecom industry in India with globalisation and digitisation has created many security concerns in field of telecom industry as given follow.

- **Cyber security:** With development of IoT & Big Data, security challenges in telecom industry, banking and financial transactions have increased manifold like data protection, architecture, email security, web security, information security, cloud security etc.
    - According to the industry report, **only 50% of Indian companies have their security strategy for cloud computing**.
- **National security:** Data sovereignty of strategic sectors are much important in respect of national security.
    - Virtual world is increasingly being targeted in covert state-sponsored attacks and actions of non-state actors, which creates threat to the sovereignty and integrity of India.
- **Dubious suppliers:** There are dubious telecom equipment suppliers, whose products have been suspected of being misused.
    - Hence, identifying trusted source and negative list of vendors by govt will make procurement more transparent and eliminate dubious foreign suppliers.
- **Realizing Self-reliance (Atmanirbhar Bharat mission):** Currently, India is heavily dependent on import of telecom equipment at Rs 1.30 trillion and China is biggest exporter.
    - Hence, steps towards telecom security with given directives will help to include more domestic trusted sources, which ultimately helps in boosting India's domestic capacities and reduce reliance on foreign equipment.

**Ways to address challenges in telecom security**

It is said that with list of banned sources and limited trusted sources **makes price of telecom equipment higher or uncompetitive.** E.g. Equipment sold by Ericsson, Nokia and Samsung are relatively expensive and may add to input cost. Hence, security in telecom industry can be improved by other measures as well.

- **Technological advancements:** For this the C-DOT, telecom research and development arm of govt should work for development of technology and products.
- **Strategy and approach:** Adopting a holistic and strategic approach to deal with security vulnerabilities as given below.
    - **Threat detection:** It is the practice of analyzing the entirety of a security ecosystem to identify any malicious activity that could compromise the network and help neutralize the threat before it can exploit any present vulnerabilities.
    - **Prevention measures:** Here the legal frameworks come into force and legal security measures are created by the regulators and the sectors, in order to overcome security concerns.
    - **Incident response methods**: It is structured methodology for handling security incidents, breaches, and cyber threats with well-defined incident response plan (IRP).

## 5.1.2. CYBER-NUCLEAR SECURITY ARCHITECTURE

**Why in news?**

With, recent incidences of attacks on critical infrastructure including the nuclear reactors there is a growing concern among experts on evaluating the current state of cyber security in India's civilian and military nuclear systems.

**More on news**

- Over the years, India's nuclear infrastructure becomes increasingly more integrated with cyber technologies, which has made the likelihood of a cyber or blended attack more likely.
- In late 2019, the Kudankulam nuclear power plant in Tamil Nadu suffered breaches in their security. A large amount of data had been taken from the administrative network, implying the possibility of future attacks on more critical systems at the plant.

**Consequences of Cyber Attacks on Nuclear Facilities**

- **Theft of sensitive and confidential information** about nuclear facilities, reactor designs etc.
- **Risks of hacking, disruption, and potential for sabotage:** Unauthorised access to the command and control infrastructure of a nuclear weapons system may defeat the security of the weapons and possibly conduct an unauthorised launch or use of nuclear warheads or missiles.
    - For instance, the **attack on the Natanz nuclear facility (Iran)** in 2021 targeted the industrial control systems and destroyed the power supply to centrifuges used to create enriched uranium.
- **Theft of nuclear/radioactive materials** and radiation release due to malicious intent of adversaries.
- **Creates Distrust:** A cyber-attack on a specific component exposes vulnerabilities in the entire system which may negatively impact relations with allies and adversaries and questions our nuclear reliability.

**Existing challenges in dealing with cyber threats in nuclear domain**

- **National Cyber Security Policy, 2013, lacks in any explicit mention** of the correlation between cyber and nuclear security.
- **No mechanism in place where the public can be informed of any breach** of the country's cyber and nuclear infrastructure. As a result, cyber threats remain unrecognised and unresolved.
- **Lack of inter-agency coordination** in developing countermeasures as well as a gap in information-sharing.

**Way ahead**

Given the sensitive nature of nuclear materials and infrastructure, it is important to create policies that offer short-term and long-term solutions with changing security needs. This includes:

- **Identifying threats:** It is vital to analyze vulnerabilities that the systems protecting the country's nuclear facilities may be susceptible to.
    - Looking at notable incidents of cyber breaches at nuclear systems and the lessons learned would provide useful insights to avoid similar threats for India.

- **Updating the policy:** A new Cyber Security Policy is expected to be released in 2020. It must fill the inadequacies in the current one, to address the evolving challenges to cyber security in the nuclear domain.
- **Engaging in multilateral dialogues** to help develop appropriate international regulatory frameworks, norms and institutions for cyber and nuclear security.
    - In bilateral terms, India could work with partners and allies like Japan and Australia to facilitate cooperation and promote sharing of best practices in this domain.
- **Resilience of supply chain:** Strong policies should be adopted in terms of sourcing, vendor management, supply chain continuity and quality.

**Conclusion**

Given the rapid nature of technological advancements, cyber security should be a key consideration while modernising nuclear systems and facilities.

## 5.2. CYBER SURVEILLANCE

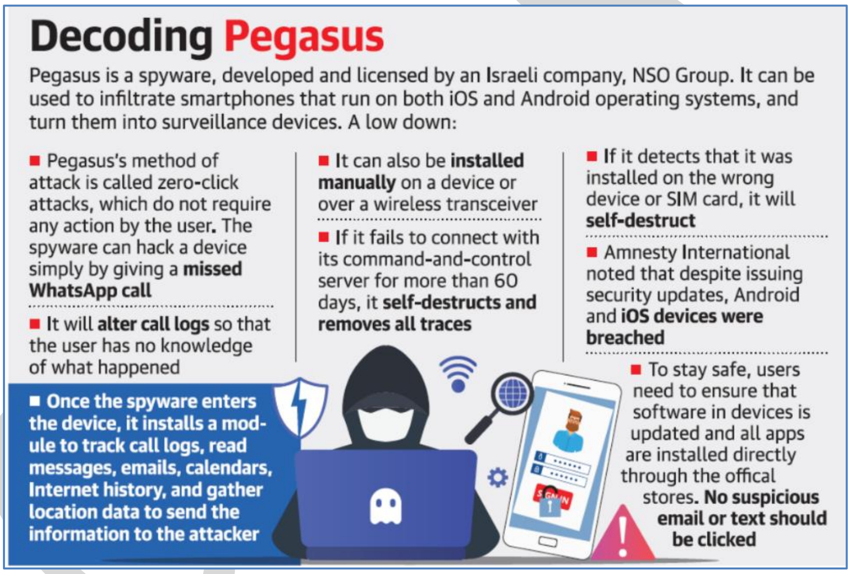
**Facial recognition**

**Why in news?**

Recent controversy regarding **Pegasus spyware** has fuelled the debate related to cyber surveillance in India.

**What is cyber surveillance and its laws in India?**

- Surveillance means **close observation of a person or groups who are under suspicion** or the act or the condition of being observed.
- Cyber-surveillance is when a person uses **"smart" or "connected" devices that communicate through a data network to monitor people or places**. This type of connected technology has also been called the **"Internet of Things" (IoT).** Devices used for cyber-surveillance are generally connected to each other and to a device or app that can control them.

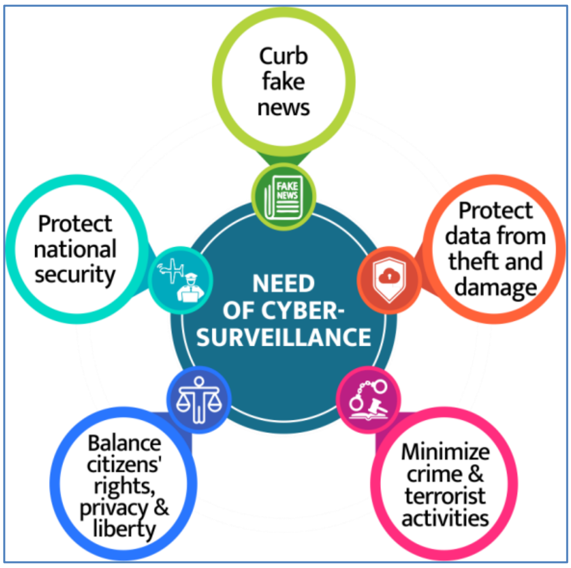


**Decoding Pegasus**

Pegasus is a spyware, developed and licensed by an Israeli company, NSO Group. It can be used to infiltrate smartphones that run on both iOS and Android operating systems, and turn them into surveillance devices. A low down:

- Pegasus's method of attack is called zero-click attacks, which do not require any action by the user. The spyware can hack a device simply by giving a **missed WhatsApp call**
- It will **alter call logs** so that the user has no knowledge of what happened
- **Once the spyware enters the device, it installs a module to track call logs, read messages, emails, calendars, Internet history, and gather location data to send the information to the attacker**
- It can also be **installed manually** on a device or over a wireless transceiver
- If it fails to connect with its command-and-control server for more than 60 days, it **self-destructs and removes all traces**
- If it detects that it was installed on the wrong device or SIM card, it will **self-destruct**
- Amnesty International noted that despite issuing security updates, Android and **iOS devices were breached**
- To stay safe, users need to ensure that software in devices is updated and all apps are installed directly through the offical stores. **No suspicious email or text should be clicked**

- **Communication surveillance in India** takes place primarily **under two laws:**
    - **The Indian Telegraph Act, 1885: Section 5** of the act had given power to central or state government to **intercept any message/calls in two circumstances, if it is:**
        - ✓ Against **public safety or public emergency.**
        - ✓ Necessary in the **interests of the sovereignty and integrity of India**; the **security of the State; friendly relations with foreign states** or **public order**; for **preventing incitement** to the commission of an offense.
        - ✓ Same restrictions are also imposed on free speech under Article 19(2) of the Constitution.
    - **Information Technology (IT) Act, 2000:** It was enacted to provide legal recognition for electronic communication, electronic commerce and cybercrimes etc.
        - ✓ **Section 69** of the **IT Act and the IT (Procedure for Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009** were enacted to deal with **surveillance of all electronic communication**.
        - ✓ IT Act covers the civil and criminal offences of **data theft and hacking.**


Curb fake news
FAKE NEWS
Protect national security
Protect data from theft and damage
NEED OF CYBER-SURVEILLANCE
Balance citizens' rights, privacy & liberty
Minimize crime & terrorist activities

**Concerns associated with Cyber- Surveillance**

- **Threat to press freedom**: The **personal safety of journalists and their sources** especially those whose work criticises the government is jeopardised. Therefore, lack of privacy creates an aura of distrust around these journalists and effectively buries their credibility.
    - **World Press Freedom Index** produced by 'Reporters without Borders' has r**anked India 142 out of 180 countries** in 2021.
- **Right to privacy and free speech**: The perceived danger founded on reasonable suspicion **impacts citizens' ability to express, receive and discuss unorthodox, controversial or provocative ideas.**
- **Absence of oversight:** Due to lack of parliamentary or judicial oversight, electronic surveillance **gives power to executive to** exercise disproportionate amount of power, encouraging **spread of authoritarianism.**
- **Violates due process of law:** When surveillance are carried out by the executive, it **curtails Articles 32 and 226 of the constitution** (empowering the Supreme Court and High Courts, respectively, to issue certain writs) as it happens in secret. Thus, the affected person is unable to show a breach of their rights.
    - This **violates not only the ideals of due process and the separation of powers** but also goes against the requirement of procedural safeguards as mandated in K.S. Puttaswamy (Retd) v. Union of India (2017).

**State backed surveillance vs. Right to privacy**

- The Supreme Court (SC) of India pronounced its judgment in the case of **People's Union for Civil Liberties (PUCL) vs Union of India (1997)**, which laid the groundwork for the right to privacy in the context of telephonic surveillance (i.e. wiretaps) and constitutional freedom.
- The SC in a landmark decision in **KS Puttaswamy versus Union of India (2017)** unanimously **upheld right to privacy as a fundamental right** under Articles 14, 19 and 21 of the Constitution.
    - Telephone tappings and internet hacking by State, of personal data falls within the realm of privacy.
- Privacy judgment lays down **four-fold test that needs to be fulfilled** before state intervention in the right to privacy:
    - State action must be sanctioned by law
    - In a democratic society, there must be a legitimate aim for action
    - Action must be proportionate to the need for such interference
    - It must be subject to procedural guarantees against abuse of the power to interfere
- Bombay High Court in **Vinit Kumar vs Central Bureau of Investigations and Ors (2019),** outlined the ambit of state's power to surveil its subjects particularly on matters that do not fall within the category of 'public emergency' or 'in the interest of public safety'.

- **Threat to National security: Increasing Cyber-terrorism and cyber-crimes** penetration motivated the attack against information, computer systems and programs and data which **results in violence against non-combatant targets by sub-national groups** or secret agents.

**Way forward**

- **Role of Judiciary**: Judicial oversight is necessary to decide whether specific instances of surveillance are proportionate, whether less onerous alternatives are available, and to **balance the necessity of the government's objectives with the rights of the impacted individuals.**
- **Awareness:** There has to be an educational framework to teach people how to identify and avoid incidents that might lead to personal and corporate data being compromised.
- **Decentralised system:** Tracking systems have to be made decentralised and open-source, and should be designed in such a way that data is shared without any privacy breach.
- **Dedicated cyber security law**: India needs to come up with **more effective legal frameworks and stringent provisions to fight cybercrime,** to protect India, its cyber security, cyber sovereign interests.
    - As per Cyber Security Summit organised by the Confederation of Indian Industry (CII), **India needs to move on from IT security to cyber security.**
- **Use of Artificial intelligence (AI)** for preventing and accurately identifying cyber-attacks and real-time threat intelligence.

## 5.2.1 FACIAL RECOGNITION TECHNOLOGY

**Why in news?**

Recently, in order to empower the Indian police with information technology, Government has approved implementation of the **National Automated Facial Recognition System (NAFRS).**

### More on news

- Facial recognition is a way of **identifying or confirming an individual's identity using their face**. Facial recognition systems can be used to identify people in photos, videos, or in real-time.
- NAFRS is to be **used by police pan-India and will be issued by the National Crime Records Bureau (NCRB).**
- It would be a **mobile and web-based application hosted in Delhi** to help in crime prevention and detection, and fast track document verification.
- It is supposed to be **interlinked with other existing databases** like Crime and Criminal Tracking Network & Systems (CCTNS), Integrated Criminal Justice System (ICJS), State-specific database systems and the Khoya-paya portal.
- **It will use facial recognition technology**: to facilitate investigation of crime or for identifying a person of interest (e.g., a criminal) regardless of face mask, makeup, plastic surgery, beard, or hair extension.

### Significance of Facial Recognition technology

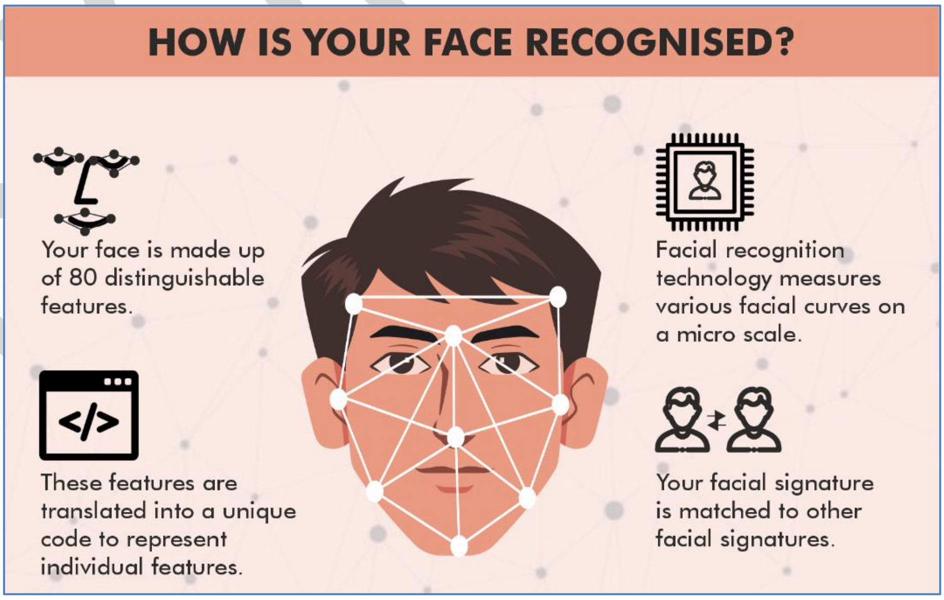
- **Increased security**: It can help to **identify terrorists or other criminals.**
- **Faster processing**: Face recognition takes only seconds, thus it enables **quick and efficient verification** of a person's identity.
- **Reduced crime**: The sole knowledge of the presence of a face recognition system can serve as deterrence, especially to petty crime.
- **Removing bias from stop and search**: By singling out suspects among crowds through an automated rather than human process, face recognition technology could help **reduce potential bias** and decrease stops and searches on law-abiding citizens.

**Mechanisms of some of the identification methods-**

- **Fingerprint:** Fingerprints are easy to capture, and can verified by comparing the unique loops, arches, and whorls in each pattern.
- **Voice Recognition:** Physically, the shape of a person's vocal tract, including the nose, mouth, and larynx determines the sound produced. Behaviorally, the way a person says something – movement variations, tone, pace, accent, and so on – is also unique to each individual.
- **Retina Scan:** Retinal scans capture capillaries deep within the eye (unique to each person) by using unique near-infrared cameras.
- **Keystroke dynamics:** Keystroke dynamics leverage the fact that people follow a definite pattern while typing on a keyboard or keypad.
- Apart from the aforementioned indicators, other biometrics are also emerging like ear authentication, footprint and foot dynamics and gait recognition (style of walking).

### Challenges associated with technology

- **Scope for error:** It 'identifies' or 'verifies' only in probabilities (e.g., 70% likelihood that the person shown on an image is the same person on a watch list).
  - For instance, there is a **possibility of producing 'false positives'** — a situation where the algorithm finds an incorrect match, even when there is none — resulting in wrongful arrest.



HOW IS YOUR FACE RECOGNISED?

Your face is made up of 80 distinguishable features.

Facial recognition technology measures various facial curves on a micro scale.

These features are translated into a unique code to represent individual features.

Your facial signature is matched to other facial signatures.

- **Inherent biasness**: Research suggests facial recognition software is based on pre-trained models. Therefore, if certain types of faces (such as female, children, and ethnic minorities) are under-represented or over-represented in training datasets, then this bias will negatively impact its performance.
  - For instance, with the element of error and bias, facial recognition can result in profiling of some overrepresented groups (such as Dalits and minorities) in the criminal justice system.
- **Massive data storage**: Facial recognition software relies on machine learning technology, which requires massive data sets to "learn" to deliver accurate results. Such large data sets require robust data storage.

- **Impact on right to privacy**: As NAFRS will collect, process, and store sensitive private information: facial biometrics for long periods; if not permanently — it will impact the right to privacy.
    - **NAFRS fails each one of the three tests** (existence of law, guarantee against arbitrary state action and a rational nexus between objectives and means to achieve them) given by **Supreme Court in Justice K.S. Puttaswamy vs Union of India (2017) case.**
- **Lack of Research & Development**: Policing and law and order being State subjects, some Indian States have started the use of new technologies without fully appreciating the dangers involved.
- **Impacts Liberal Democracy**: As anonymity is key to functioning of a liberal democracy, unregulated use of facial recognition technology will dis-incentivise independent journalism or the right to assemble peaceably without arms, or any other form of civic society activism.

**International practices**

- **United States:** The Federal Bureau of Investigation uses facial recognition technology for potential investigative leads.
- **United Kingdom:** police forces in England use facial recognition to tackle serious violence.
- **China:** It uses facial recognition for racial profiling and mass surveillance in order to track Uighur Muslims.

**Way forward**

- **Need of a clear law**: In the interest of civil liberties and to save democracy from turning authoritarian, it is important to enact a strong and meaningful data protection law, in addition to statutory authorisation of NAFRS and guidelines for deployment.
- **Required Expertise in the field**: The data collected from social media profiles has risk involved related to the authenticity of the data. Hence, experts are needed to verify such details before storing them who should be provided proper training to protect & avoid abuse and misuse of the collected data & database.
- **Adequate safeguards**: such as penalties, along with enhanced accountability of the law enforcing bodies and adequate oversight, to minimize the potential for misuse and abuse of the facial recognition technology.

# 6. INSURGENCY IN THE NORTH EAST

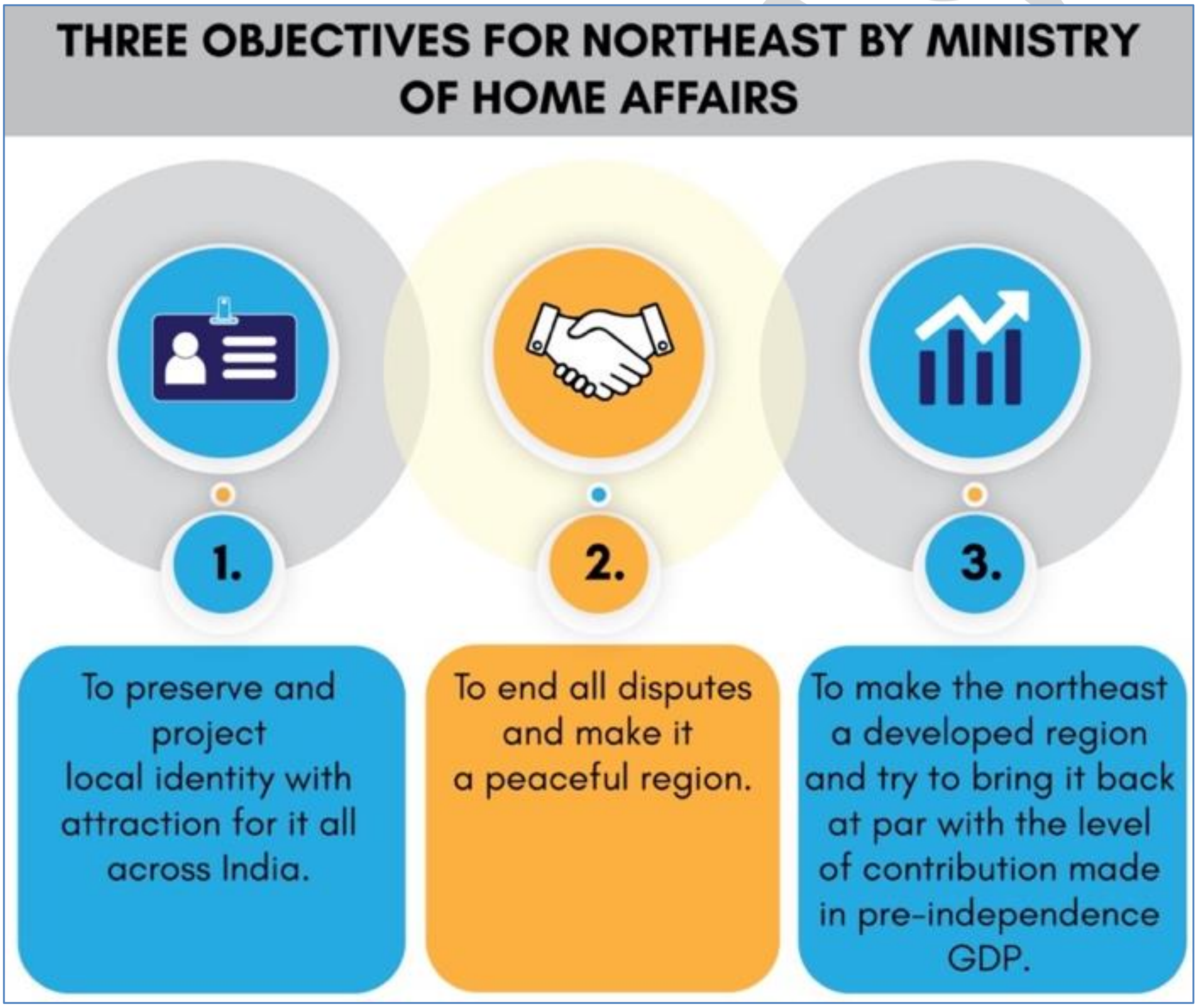
**Overview**

There are over a hundred of ethnic groups in the Northeast each having a strong sense of identity and their uniqueness. They want to retain this uniqueness in their political and social and orientations as well. Insurgency is essentially a violent rebellion against the political organisation when the ethnic communities feel that their interests have been neglected and they are not properly represented.

The large prevalence of insurgency has negatively impacted the prevalence of Peace in the Northeast. This not only affects the socio-economic development of the region but has a negative effect on the country as well.

**Status at present**

However, through **ceasefire agreements**, **peace talks**, strong **military actions** within India, the Northeast region is witnessing a drastic decline in insurgency in the last 5 to 6 years. As **compared to 2014, insurgency came down by 80% in 2020** with 162 incidents and 2 civilians being killed. Still many insurgent groups are still active in the region.

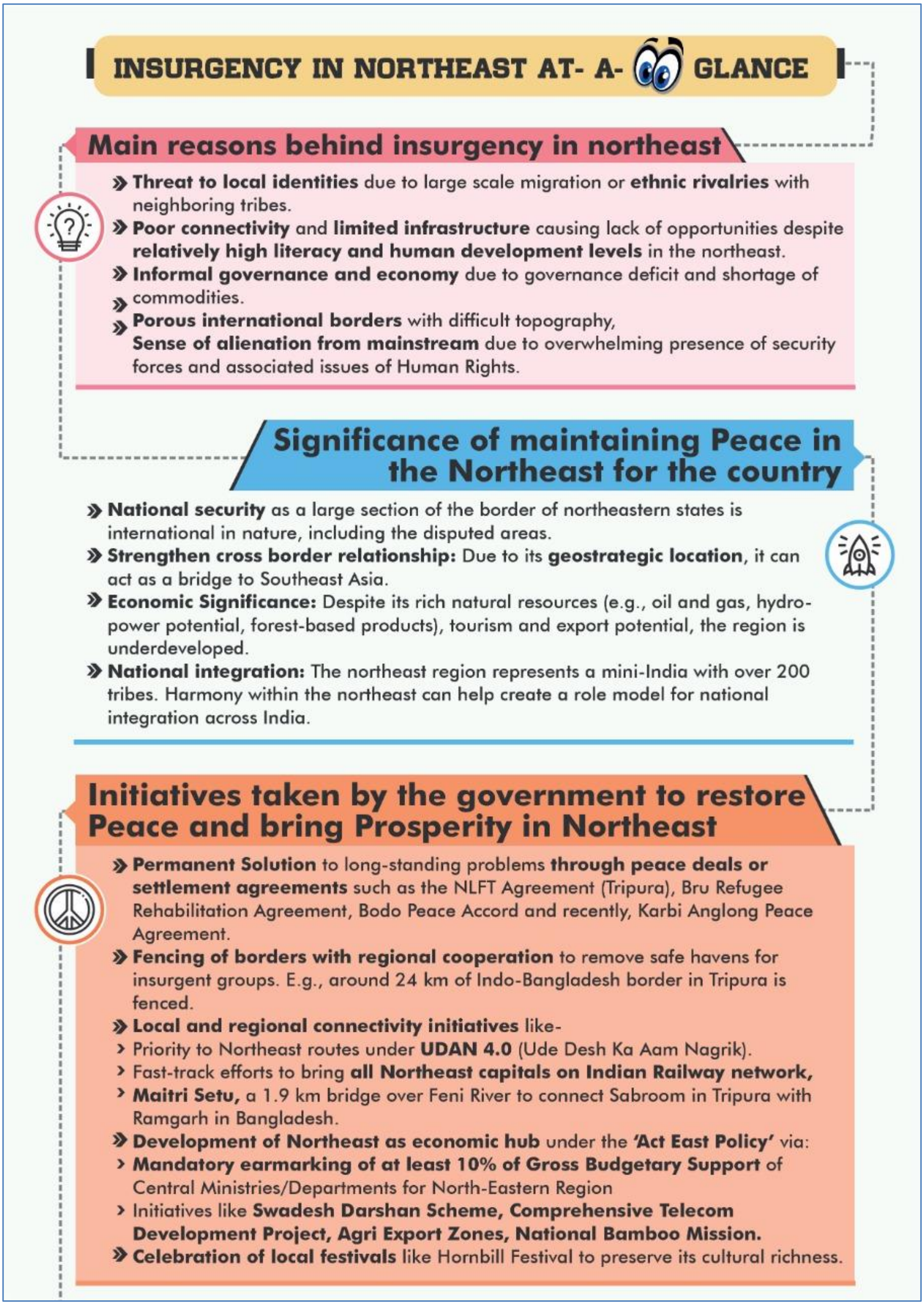


THREE OBJECTIVES FOR NORTHEAST BY MINISTRY OF HOME AFFAIRS

1. To preserve and project local identity with attraction for it all across India.

2. To end all disputes and make it a peaceful region.

3. To make the northeast a developed region and try to bring it back at par with the level of contribution made in pre-independence GDP.



# INSURGENCY IN NORTHEAST AT- A- GLANCE

## Main reasons behind insurgency in northeast

- **Threat to local identities** due to large scale migration or **ethnic rivalries** with neighboring tribes.
- **Poor connectivity** and **limited infrastructure** causing lack of opportunities despite **relatively high literacy and human development levels** in the northeast.
- **Informal governance and economy** due to governance deficit and shortage of commodities.
- **Porous international borders** with difficult topography,
- **Sense of alienation from mainstream** due to overwhelming presence of security forces and associated issues of Human Rights.

## Significance of maintaining Peace in the Northeast for the country

- **National security** as a large section of the border of northeastern states is international in nature, including the disputed areas.
- **Strengthen cross border relationship:** Due to its **geostrategic location**, it can act as a bridge to Southeast Asia.
- **Economic Significance:** Despite its rich natural resources (e.g., oil and gas, hydro-power potential, forest-based products), tourism and export potential, the region is underdeveloped.
- **National integration:** The northeast region represents a mini-India with over 200 tribes. Harmony within the northeast can help create a role model for national integration across India.

## Initiatives taken by the government to restore Peace and bring Prosperity in Northeast

- **Permanent Solution** to long-standing problems **through peace deals or settlement agreements** such as the NLFT Agreement (Tripura), Bru Refugee Rehabilitation Agreement, Bodo Peace Accord and recently, Karbi Anglong Peace Agreement.
- **Fencing of borders with regional cooperation** to remove safe havens for insurgent groups. E.g., around 24 km of Indo-Bangladesh border in Tripura is fenced.
- **Local and regional connectivity initiatives** like-
  - Priority to Northeast routes under **UDAN 4.0** (Ude Desh Ka Aam Nagrik).
  - Fast-track efforts to bring **all Northeast capitals on Indian Railway network,**
  - **Maitri Setu,** a 1.9 km bridge over Feni River to connect Sabroom in Tripura with Ramgarh in Bangladesh.
- **Development of Northeast as economic hub** under the **'Act East Policy'** via:
  - **Mandatory earmarking of at least 10% of Gross Budgetary Support** of Central Ministries/Departments for North-Eastern Region
  - Initiatives like **Swadesh Darshan Scheme, Comprehensive Telecom Development Project, Agri Export Zones, National Bamboo Mission.**
- **Celebration of local festivals** like Hornbill Festival to preserve its cultural richness.

## Challenges to Peace and Prosperity Initiatives

- **Presence of un-demarcated borders** with difficult terrain, making fencing of borders a complex task.
- **Natural challenges to the economic development and connectivity** initiatives from hazard risks, presence of ecologically sensitive areas and difficulties in land-acquisition,
- **Limited FDI inflows and predominance of Informal Economy** in Northeast.
- **The presence of organized crime syndicates** involved in human-trafficking, narcotics trading, poaching etc.
- **Slowdown in Indian trade** growth with ASEAN nations and **attack on Indian connectivity projects** in Myanmar, by rebel groups creating challenge to Act East Policy.
- **Prevailing stereotypes** about people and region among people from other regions.

## Way Forward

- **At Socio-cultural Level,** increase awareness on culture, language, and people of Northeast among rest of Indians and outside.
- **At Economic Level,** working on light industries such as food processing, floriculture, sericulture etc. in proximity with existing infrastructure to build necessary entrepreneurship in the region.
- **At National Security Level,** continue with peace efforts with continued counter insurgency operations while respecting human rights.
- **At International Level,** sorting out un-demarcated border issues to overcome porous border issues with joint efforts against insurgent groups and organized crime syndicates operating from neighboring nations.
- **At Political Level,** engaging the Northeastern political parties and civil society for social integration in the region.

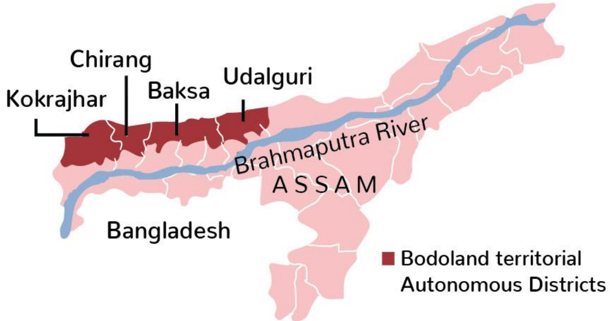
## 6.1. BODO PEACE ACCORD

**Why in News?**

Recently, first anniversary of the 3rd Bodo Peace Accord was celebrated in Assam recently.

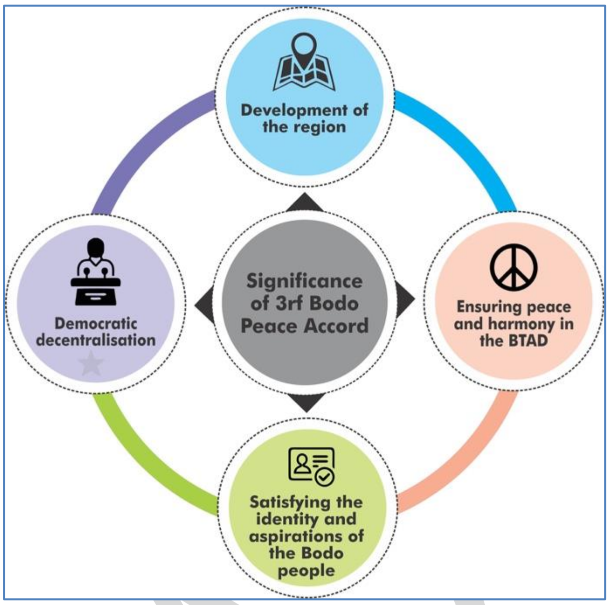
**About 3rd Bodo Peace Accord**

- 3rd Bodo Peace Accord as **tripartite agreement between the Centre, Assam Government and the banned Assam- based insurgent group National Democratic Front of Bodoland (NDFB)** was signed on 27th January 2020, for bringing a lasting peace in Bodo-dominated areas in Assam.
- **Key highlights of the accord**
  - **Bodo Territorial Areas District (BTAD)** was reorganized by including new **Bodo-dominated villages contiguous to the existing BTAD and excluding villages with a predominantly non-tribal population.**



**Timeline of the Bodoland dispute**

- **1960s and 1970s** - There were calls from Bodos and other tribes for a separate state of 'Udayachal' as immigrants were accused of illegally encroaching on Bodo-inhabited lands. Demand was raised under the banner of the Plains Tribals Council of Assam (PTCA), a political outfit.
- **1993** - The Bodoland Autonomous Council (BAC) was constituted after the Centre, the Assam government and the All-Bodo Students Union (ABSU) signed a tripartite agreement. However, BAC failed due to non-implementation of various provisions of the Accord.
- **2003** - The Bodoland Territorial Council (BTC) was formed after the Centre; the Assam government and the BLT sign a tripartite agreement. The BLT is disbanded.
- **2005** – NDFB agreed to a ceasefire with the Assam government and the Centre. After the treaty was signed, the group splits into three factions. One of those factions, the NDFB (S) continued to carry out violent attacks.


Significance of 3rf Bodo Peace Accord
Development of the region
Ensuring peace and harmony in the BTAD
Satisfying the identity and aspirations of the Bodo people
Democratic decentralisation

- **BTAD renamed as Bodoland Territorial Region(BTR)** with more executive, administrative, legislative and financial powers.
- **A commission,** headed by a neutral person and represented by stakeholders, **will be constituted by the central government for the demarcation and reorganisation of the BTR**
- Bodos living in hills districts of Karbi Anglong and Dima Hasao would **be conferred Scheduled Hill Tribe status.**
- **Number of seats in Bodoland Territorial Council will be increased** from 40 to 60.
- **Bodo with Devnagri script would be associate official language** for entire Assam.
- Deputy Commissioners and Superintendents of Police will be posted in consultation with the Chief Executive Member (CEM) of the BTC.
- **A Special Development Package of Rs. 1500 crores** over three years were provided.

**Progress so far**

- **Boundary commission has been formulated** to give a new shape to the BTR,
- Development work for the residents of the Bodo region is being done through various commissions and advisory committees.
    - **65 schemes worth Rs. 750 crore have been commissioned**, and a separate allocation of Rs. 565 crore has also been done.
- **Assam Official Language (Amendment) Bill, 2020 passed** to give due respect to the Bodo language,
- **Assistance of Rs. 4 lakh has been started for all surrendered militants.**

# 7. MISCELLANEOUS

## 7.1. INTELLIGENCE REFORMS

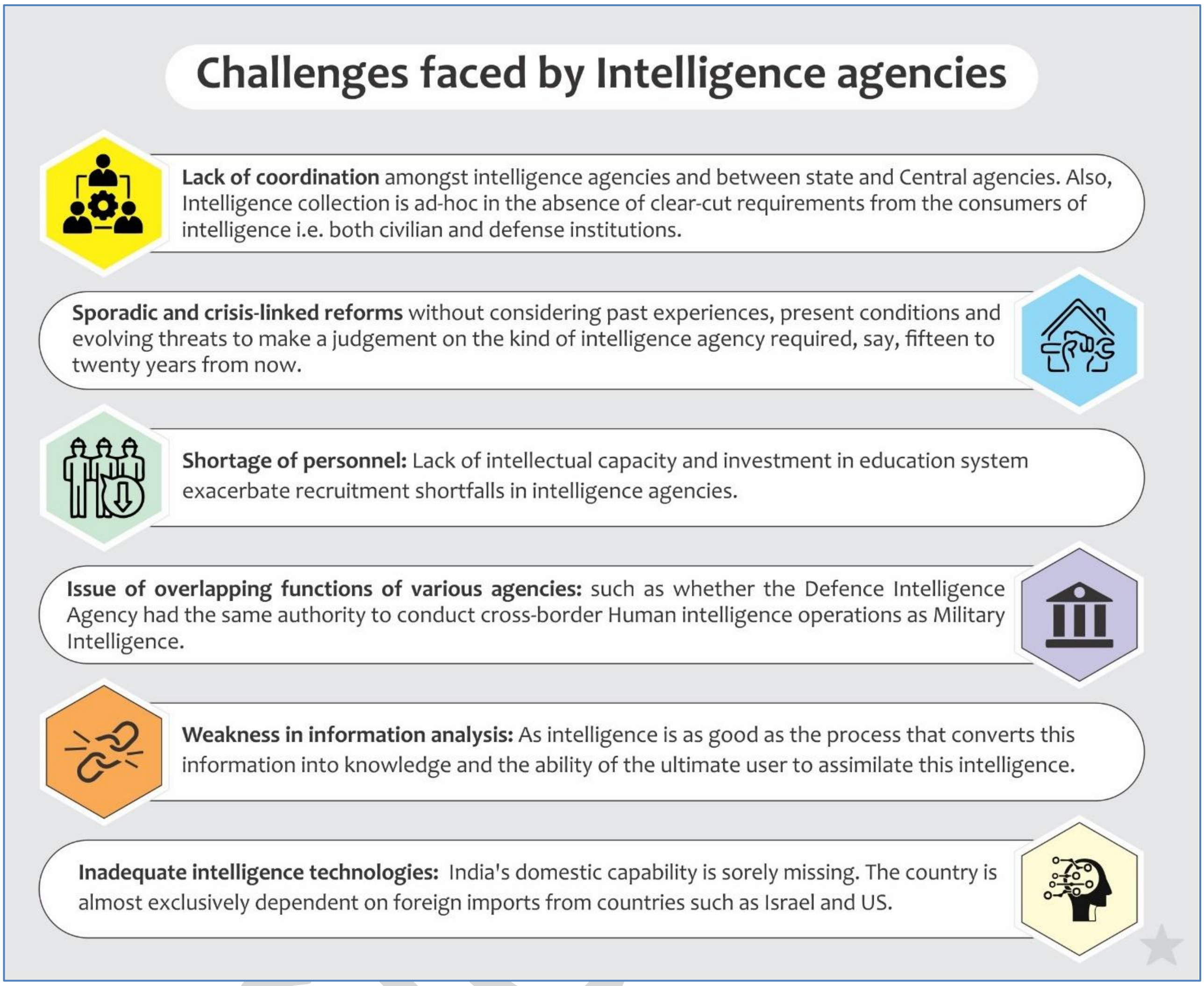
**Why in News?**

In the backdrop of repeated China's incursions, experts have called for intelligence reforms.

**Intelligence Framework in India**

- India's existing intelligence apparatus **comprises an assortment of agencies** that have specific mandates.
- At the apex level, the **National Security Council Secretariat (NSCS),** headed by the National Security Advisor (NSA), was set up by the government following the 1998 Pokhran-II nuclear tests.
    - It operates within the executive office of the Prime Minister of India, **liaising between the government's executive branch and the intelligence services,** advising leadership on intelligence and security issues.
- In 2018, the **Joint Intelligence Committee (JIC),** a body created to aggregate and analyse all intelligence from the various agencies, was subsumed into the NSCS.
- **Various Intelligence agencies**
    - **IB,** created in 1887, reports to the Ministry of Home Affairs and is responsible for India's domestic intelligence, internal security, and counter-intelligence.
        - ✓ It was first named Indian Political Intelligence Office and it was given its current name after Independence.
    - **Research and Analysis Wing (R&AW),** meanwhile, is the country's foreign intelligence agency formed in 1968.
        - ✓ It comes under the direct command of the prime minister. R&AW is a wing of the Cabinet Secretariat.
    - **National Technical Research Organisation** (NTRO; erstwhile National Technical Facilities Organisation): It was established in 2004 and is the technical intelligence agency of the Government of India.
        - ✓ NTRO comes under the National Security Advisor and is part of the Prime Minister's Office.
    - **Directorate of Revenue Intelligence (DRI):** It is tasked with anti-smuggling intelligence; it was set up in 1957, and falls under the Ministry of Finance.
- The "norms of conduct" of the IB, R&AW and NTRO are governed by the **Intelligence Organisations (Restrictions of Rights) Act, 1985.**
    - Additionally, employees of Indian intelligence agencies are **subject to the Official Secrets Act (first enacted in 1923)** that governs, among others, the sharing of classified information.

**Diverse and complex national security threats** range from nuclear-armed adversaries like China and Pakistan, to Maoists to cyber terrorism **calls for the need for Intelligence reforms.**



## Challenges faced by Intelligence agencies

**Lack of coordination** amongst intelligence agencies and between state and Central agencies. Also, Intelligence collection is ad-hoc in the absence of clear-cut requirements from the consumers of intelligence i.e. both civilian and defense institutions.

**Sporadic and crisis-linked reforms** without considering past experiences, present conditions and evolving threats to make a judgement on the kind of intelligence agency required, say, fifteen to twenty years from now.

**Shortage of personnel:** Lack of intellectual capacity and investment in education system exacerbate recruitment shortfalls in intelligence agencies.

**Issue of overlapping functions of various agencies:** such as whether the Defence Intelligence Agency had the same authority to conduct cross-border Human intelligence operations as Military Intelligence.

**Weakness in information analysis:** As intelligence is as good as the process that converts this information into knowledge and the ability of the ultimate user to assimilate this intelligence.

**Inadequate intelligence technologies:** India's domestic capability is sorely missing. The country is almost exclusively dependent on foreign imports from countries such as Israel and US.

### Way forward

- **Better coordination:** Appoint a National Intelligence Coordinator/Director of National Intelligence to bring about better interagency coordination, remove overlaps and duplications, end 'turf-wars' and ensure better utilisation of national resources.
- **Providing legal status:** That would give India's intelligence community a statutory basis and a charter, and will provide it with institutional levels of accountability.
- **Improving accountability:** Strengthen financial accountability by annual reports to Comptroller & Auditor General (CAG)/NSA, a separate intelligence ombudsman, setting up a Parliamentary Accountability Committee for oversight of intelligence agencies etc.
- **Robust base in technology and innovation:** Such a framework will need a tripartite partnership between government, private sector and the academia. There is a need to identify specific technology pathways and create a concrete five-year plan to swiftly build local capacity.
- **Reforms in recruitment, deputation, promotion and training:** By having open and separate direct recruitment mechanisms for different intelligence agencies, improving training modules, improving quality of trainers and in situ promotions to improve morale at middle, mid-senior levels.
- **Gathering information from open sources:** Information is emanating not only from traditional media sources such as newspapers, magazines and television, but also social media like micro-blogs, Twitter and Facebook.
- **Capacity for analyzing gathered information:** There is need for the system to separate collection and analysis of intelligence while strengthening both these functions.

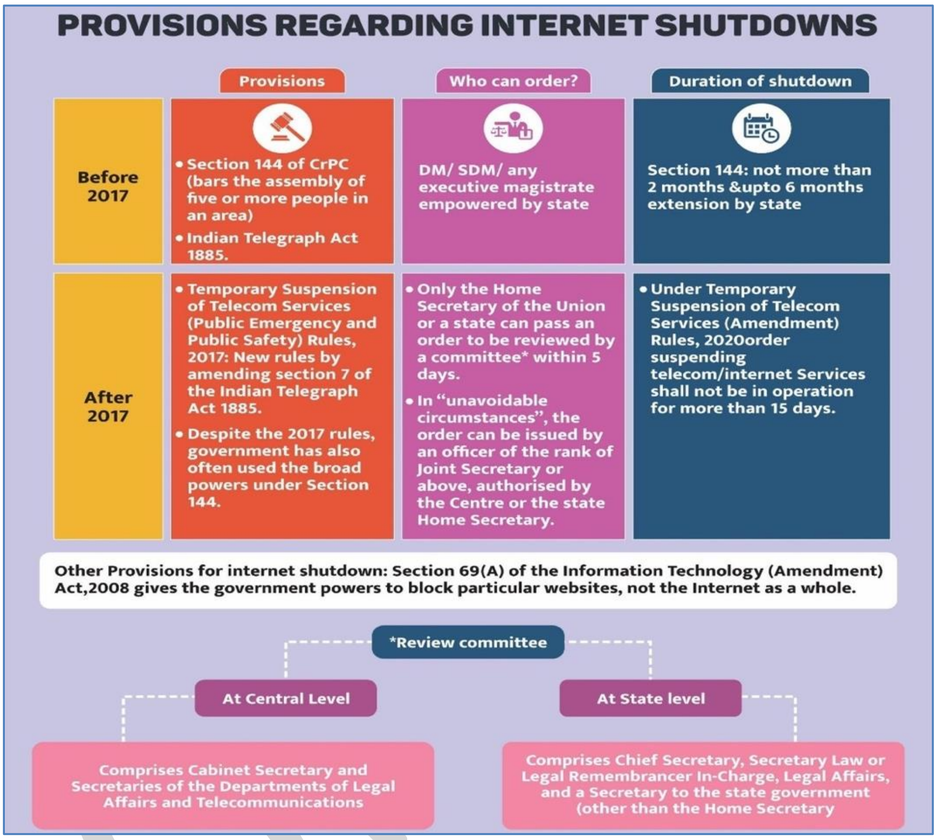
## 7.2. INTERNET SHUTDOWNS

**Why in News?**

As per a recent report by UK-based privacy and security research firm Top10VPN, **Internet shutdowns in 2020 cost India $2.8 bn,** almost 70% of the total loss of $4 bn to the world economy.

**About Internet Shutdown**

- **Definition:** Internet shutdown as an **intentional disruption of internet** or electronic communications for a specific population or location, to exert control over the flow of information. It can be caused by **internet blackouts, social media shutdowns** or **throttling** where access to the internet is reduced to 2G speeds.
- **Argument in favor of Internet shutdowns:** Ensure peace and public stability by acting as an instrument to prevent hate speech, fake news, etc.



PROVISIONS REGARDING INTERNET SHUTDOWNS

| | Provisions | Who can order? | Duration of shutdown |
|---|---|---|---|
| Before 2017 | • Section 144 of CrPC (bars the assembly of five or more people in an area)<br>• Indian Telegraph Act 1885. | DM/ SDM/ any executive magistrate empowered by state | Section 144: not more than 2 months &upto 6 months extension by state |
| After 2017 | • Temporary Suspension of Telecom Services (Public Emergency and Public Safety) Rules, 2017: New rules by amending section 7 of the Indian Telegraph Act 1885.<br>• Despite the 2017 rules, government has also often used the broad powers under Section 144. | • Only the Home Secretary of the Union or a state can pass an order to be reviewed by a committee* within 5 days.<br>• In "unavoidable circumstances", the order can be issued by an officer of the rank of Joint Secretary or above, authorised by the Centre or the state Home Secretary. | • Under Temporary Suspension of Telecom Services (Amendment) Rules, 2020order suspending telecom/internet Services shall not be in operation for more than 15 days. |

Other Provisions for internet shutdown: Section 69(A) of the Information Technology (Amendment) Act,2008 gives the government powers to block particular websites, not the Internet as a whole.

*Review committee

At Central Level

Comprises Cabinet Secretary and Secretaries of the Departments of Legal Affairs and Telecommunications

At State level

Comprises Chief Secretary, Secretary Law or Legal Remembrancer In-Charge, Legal Affairs, and a Secretary to the state government (other than the Home Secretary

- **Arguments against Internet shutdowns:** Violate Human rights by hampering civil liberties, economic loss, Fundamental services such as education, health care and other public services are held back**,**

**Way forward**

- Governments should identify best practices in addressing issues at their source, **prioritizing alternative measures to Internet shutdowns.**
- Governments need to do a **cost-benefit analysis of the impact of the cost of Internet shutdowns** before taking such action.
- Venture capitalists and investors should **incorporate Internet shutdowns as part of their risk assessment.**
- **Governments should document the reasons, time, alternatives considered**, decision-making authorities and the rules under which the shutdowns were imposed and release the documents for public scrutiny.

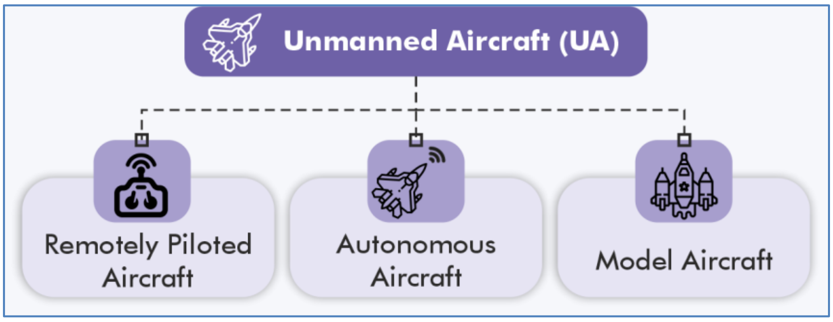
## 7.3. DRONE REGULATIONS IN INDIA

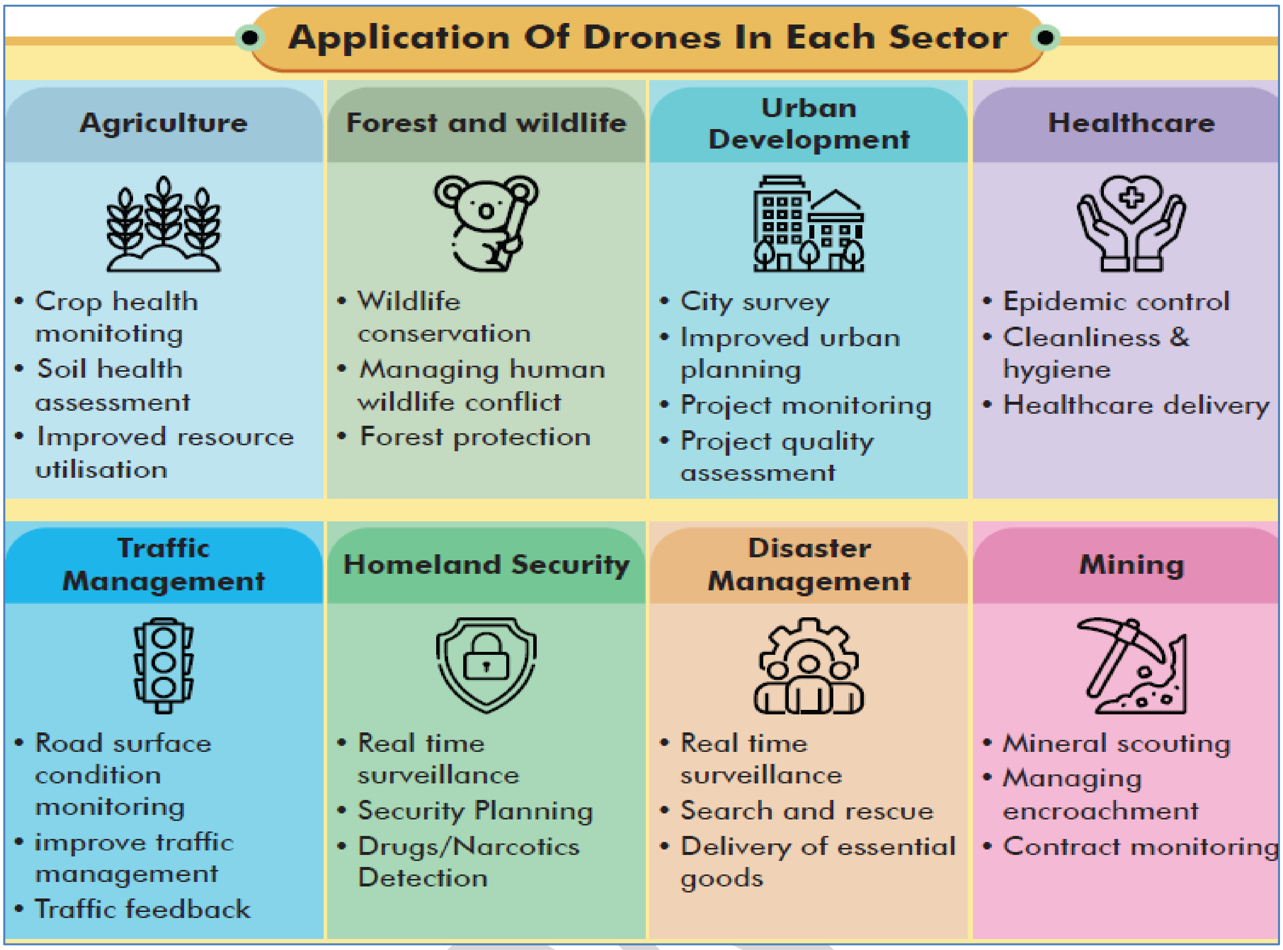
**Why in News?**

Ministry of Civil Aviation (MoCA) has released the updated – The Drone Rules, 2021 for public consultation.

**About Drones**

- Drone is a layman terminology for Unmanned Aircraft (UA), an aircraft, **which is intended to operate with no pilot on board.**
- An aircraft and its associated elements, which are operated with no pilot on board is called as Unmanned Aircraft System (UAS).





## Application Of Drones In Each Sector

| Agriculture | Forest and wildlife | Urban Development | Healthcare |
|---|---|---|---|
| • Crop health monitoting<br>• Soil health assessment<br>• Improved resource utilisation | • Wildlife conservation<br>• Managing human wildlife conflict<br>• Forest protection | • City survey<br>• Improved urban planning<br>• Project monitoring<br>• Project quality assessment | • Epidemic control<br>• Cleanliness & hygiene<br>• Healthcare delivery |
| **Traffic Management** | **Homeland Security** | **Disaster Management** | **Mining** |
| • Road surface condition monitoring<br>• improve traffic management<br>• Traffic feedback | • Real time surveillance<br>• Security Planning<br>• Drugs/Narcotics Detection | • Real time surveillance<br>• Search and rescue<br>• Delivery of essential goods | • Mineral scouting<br>• Managing encroachment<br>• Contract monitoring |

### Need of Drone regulations

- **Policy Gaps:** While the DGCA has taken the first step of framing draft guidelines for the use of UAVs, there remain several gaps that must be addressed, keeping in mind the need for balance between security concerns and legitimate uses of drones in a variety of civilian sectors.
- **Quality Control:** As a sizable percentage of India's drones continue to be imported, there is a need to ensure their quality control and standardisation.
- **The Privacy Question:** Drones can collect data and images without drawing attention, leading many citizens to fear for their right to privacy. This can also occur if government entities were to use drones to monitor the public.
- **Terrorist Threat Management:** With rapid advances in the variety of functions that a drone can undertake, there have been several instances of known terrorist organisations using them to carry out their activities. This will ensure that they do not have to resort to banning drones to deal with their potential security threats.
- **Air Traffic Management:** Drones present a new

**Drones and Security Concern**

- Security agencies in India have for some time been **anticipating the possible use of drones to target sensitive locations.**
    - A couple of years ago drones were used to drop weapons and drugs along the Punjab border.
- **Drones are becoming security threats as**
    - **Conventional radar systems are not meant for detecting low flying objects.** Besides the low altitude, what also makes it difficult to trace and intercept drones is their slow speed.
    - **Technology is easily accessible to terrorist groups** and it also provides them the capability of air strikes.
    - Drones are **relatively cheaper, compact and smaller in comparison to conventional weapons** and yet can achieve far more destructive results. There is a possible threat of them being used deliver weapons of mass destruction.
    - They **can be controlled from a remote distance** and does not endanger any member of the attacking side.
- **How India is planning to tackle the threat**
    - Defence Research and Development Organisation (DRDO) has developed an **'Anti Drone System' and it will be deployed this year.**
    - **Indian Air Force has decided to procure Counter Unarmed Aircraft System (CUAS)** that can be armed with laser directed energy weapons to bring down rogue drones.

dimension in the management of air traffic as they are neither as easy to track as conventional aircraft nor as easy to communicate with.

**Draft Drone Rules, 2021**

- Drone Rules, 2021 will replace the **Unmanned Aircraft Systems (UAS) Rules 2021** (released on 12 March 2021).
- Objective is to **enable more types of unmanned aircraft operational scenarios, increase the ease of compliance for the unmanned aviation industry, and ensure safety and security.**

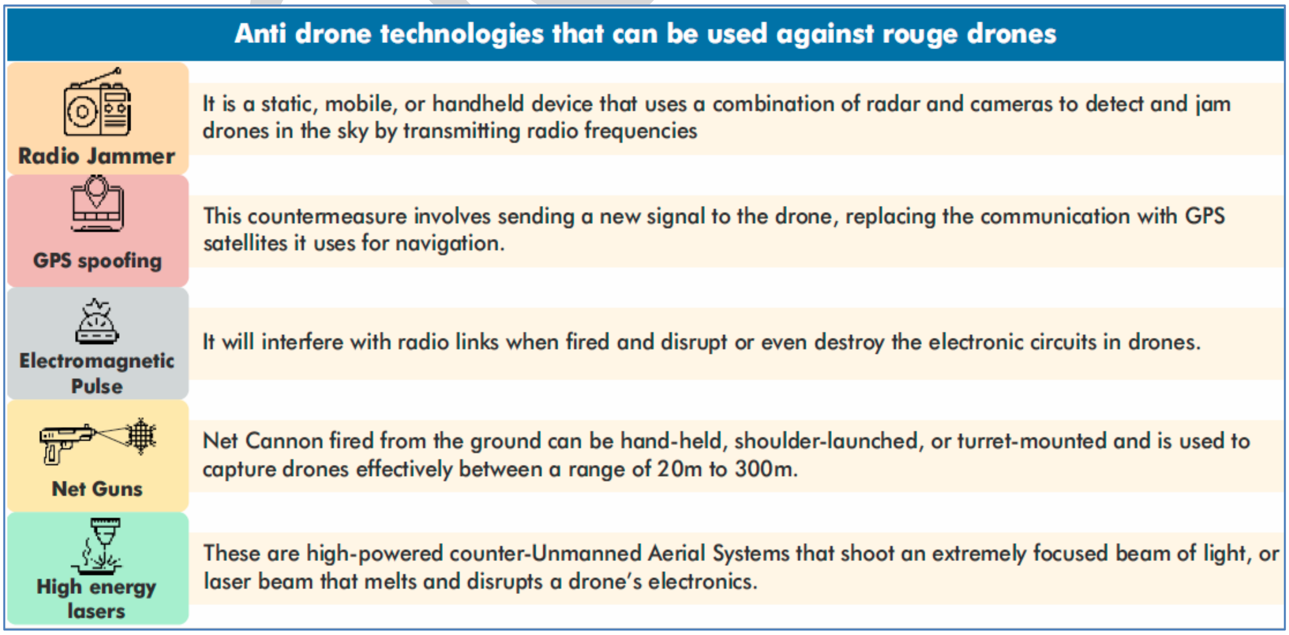
**Key provisions**

<table>
<tr><td><b>Rules will apply to</b></td><td colspan="3">• A person owning or possessing or engaged in exporting, importing, manufacturing, trading, leasing, operating, transferring, or maintaining a drone in India.<br>• All drones that are being operated for the time being, in or over India.<br>• These <b>shall not apply to drones used by the naval, military or air force.</b></td></tr>
<tr><td><b>Eligibility conditions for authorization</b></td><td colspan="3">• <b>Following natural persons shall be eligible</b> for a remote pilot license:<br>○ <b>Not less than eighteen years of age</b> and not more than sixty-five years of age.<br>○ <b>Have passed class tenth or its equivalent</b> examination from a recognised Board.<br>○ <b>Have completed the training prescribed by the Director General</b> for the applicable class of remote pilot licence from an authorised remote pilot training organisation.<br>• <b>No licence shall be required for a person operating</b><br>○ A nano drone.<br>○ A micro drone for non-commercial purposes<br>○ For research and development (R&D) organizations operating such drones.</td></tr>
<tr><td><b>Classification of drones</b></td><td colspan="3">• Will be <b>based upon the maximum all-up weight</b> including payload:<br><table><tr><th colspan="2">Classification of UAS</th></tr><tr><td>Nano</td><td><= 250g.</td></tr><tr><td>Micro</td><td>250g - 2kg</td></tr><tr><td>Small</td><td>2 kg - 25 kg</td></tr><tr><td>Medium</td><td>25 kg - 150 kg</td></tr><tr><td>Large</td><td>>150 kg</td></tr></table></td></tr>
<tr><td><b>Drone Registration</b></td><td colspan="3">• Drone <b>operators will have to generate a unique identification number</b> of a drone by providing requisite details <b>on the digital sky platform (DSP).</b><br>○ DSP is an initiative by MoCA to provide <b>a secure and a scalable platform that supports drone technology frameworks,</b> such as NPNT (no permission, no take-off), designed to enable flight permission digitally and managing unmanned aircraft operations and traffic efficiently.</td></tr>
<tr><td rowspan="3"><b>Drone Operations</b></td><td colspan="3">• Central Government may publish on DSP, an airspace map for drone operations <b>segregating the entire airspace of India into red, yellow, and green zones.</b></td></tr>
<tr><td><b>Green Zone</b><br>• <b>Airspace from the ground up to a vertical distance of 400 feet</b> (120 metre) above ground level (AGL) that has not been designated as a red zone or yellow zone in the airspace map.<br>• <b>Airspace from the ground up to a vertical distance of 200 feet</b> (60 metre) AGL in the area located between a lateral distance of 8 kilometre and 12 kilometre from the perimeter of an operational airport.</td><td><b>Yellow Zone</b><br>• <b>Controlled airspace of defined dimensions above the land areas or territorial waters of India</b> within which drone operations are restricted and shall require permission from the concerned air traffic control authority.</td><td><b>Red Zone</b><br>• <b>Airspace of defined dimensions, above the land areas or territorial waters</b> of India, or any installation or notified port limits specified by the Central Government <b>beyond the territorial waters of India;</b> within which drone operations shall be permitted only under exceptional circumstances by the Central Government;</td></tr>
<tr><td colspan="3">• <b>No person shall operate a drone in a red zone or yellow zone</b> without prior permission.<br>• In the airspace above 400 feet AGL in a designated green zone and the airspace above 200 feet AGL in the area located between the lateral distance of 8 kilometre and 12 kilometre from the perimeter of an operational airport, the <b>provisions of yellow zone shall apply;</b><br>• State Government, UT or law enforcement agency <b>may declare a temporary red zone for a period not exceeding 48 hours at a time.</b></td></tr>
</table>

| | |
|---|---|
| | ○ Declaration shall be done by an **officer not below the rank of Superintendent of Police** or its equivalent. |
| **Drone operations for research and development (R&D)** | • **Following persons shall not require a certificate of airworthiness,** unique identification number, prior permission, and remote pilot licence for operating drones:<br>○ **R&D entities and Educational institutions** under the administrative control of, or recognised by Central Government, State Governments or UT.<br>○ **Startups** recognised by Department for Promotion of Industry and Internal Trade.<br>○ Any **drone manufacturer having a Goods and Service Tax Identification Number.**<br>• But **such drone operations must take place within a green zone** and within the premises of the person where such R&D is being carried out; or within an open area in a green zone under such person's control. |
| **Other key highlights** | • In case of a drone with maximum all-up-weight **more than 500 kilogram, the provisions of the Aircraft Rules, 1937 shall apply.**<br>• Import of drones and drone components shall be **regulated by the Directorate General of Foreign Trade.**<br>• **No security clearance required** before any registration or licence issuance.<br>• **Approvals abolished:** unique authorisation number, unique prototype identification number, certificate of conformance, certificate of maintenance, import clearance, acceptance of existing drones, operator permit, authorisation of R&D organisation, student remote pilot licence, remote pilot instructor authorisation, drone port authorisation etc.<br>• **Safety features** like 'No permission – no take-off' (NPNT), real-time tracking beacon, geo-fencing etc. **to be notified in future.**<br>• Digital sky platform shall be developed as a business-friendly single-window online system.<br>• Issuance of **Certificate of Airworthiness delegated to Quality Council of India** and certification entities authorised by it. |

**Way forward**

- **An international process to define the limits of what is acceptable with respect to the possession and use of drones** by states is urgently needed.
  - EU has also urged the promotion of an **UN-based legal framework which strictly stipulates that the use of armed drones has to respect international humanitarian and human rights law.**
- **Regulation.** Despite some initial progress in defining regulations for drones, government should come up with laws that enable innovation, but restrict infringements on privacy and misuses of airspace.
- **Rectify classification of UAS under the UAS Rules** which is weight-based classification rather than performance based.



**Anti drone technologies that can be used against rouge drones**

| | |
|---|---|
| **Radio Jammer** | It is a static, mobile, or handheld device that uses a combination of radar and cameras to detect and jam drones in the sky by transmitting radio frequencies |
| **GPS spoofing** | This countermeasure involves sending a new signal to the drone, replacing the communication with GPS satellites it uses for navigation. |
| **Electromagnetic Pulse** | It will interfere with radio links when fired and disrupt or even destroy the electronic circuits in drones. |
| **Net Guns** | Net Cannon fired from the ground can be hand-held, shoulder-launched, or turret-mounted and is used to capture drones effectively between a range of 20m to 300m. |
| **High energy lasers** | These are high-powered counter-Unmanned Aerial Systems that shoot an extremely focused beam of light, or laser beam that melts and disrupts a drone's electronics. |

# WEEKLY FOCUS: SECURITY

| ISSUE | DESCRIPTION | LEARN MORE |
|---|---|---|
| Artificial Intelligence and National Security | Artificial intelligence (AI) is a rapidly growing field of technology that is capturing the attention of commercial investors, defense intellectuals, policymakers, and international competitors alike. Recently, developments like increased use of AI in cyberattacks and growth of hybrid warfare techniques have showcased how AI can potentially affect National Security. AI presents many opportunities vis-à-vis National Security along the challenges. In this context, it becomes important for India to keep pace with the integration of technological growth and defence. | |
| India's Nuclear Doctrine | India's reiteration of its 'No-first-use' policy at the UN conference of disarmament as brought India's Nuclear doctrine in the limelight. In this context, it becomes important to understand its evolution, its current paradigm, the importance it holds for India and how it needs a review in the changing technological and geopolitical landscape. | |
| Coastal Security: State of India's Preparedness | The management of coastal security in India underwent a paradigm shift after the '26/11' Mumbai terror attacks. Over the past years, efforts to secure India's coasts have stepped up. But, are they adequate? This document aims at understanding India's approach towards coastal security as it has evolved since Independence, kinds of threats and challenges that India's coasts have been facing and the factors that have hampered the smooth and effective functioning of our coastal security apparatus. | |
| Indigenisation of Defence Industry: From Necessity to Opportunity | As India inches to achieve its rightful strategic autonomy, it needs to do much more in planting the seeds for a commercially viable and technologically robust indigenous defence industrial base. Taking stock of India's efforts towards indigenous defence manufacturing, the document examines the gaps and suggests a way ahead to build an impregnable security architecture in the country. | |

# 10 IN TOP 10 SELECTIONS IN CSE 2020

*from various programs of Vision Ias*

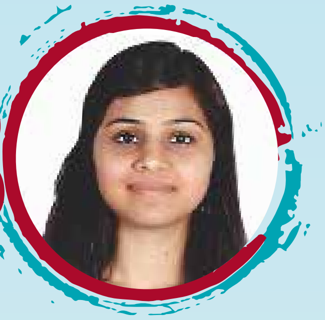
1 AIR

**SHUBHAM KUMAR**
(GS FOUNDATION BATCH
CLASSROOM STUDENT)

2 AIR

**JAGRATI AWASTHI**
(ALL INDIA
TEST SERIES )

3 AIR



**ANKITA JAIN**
(ALL INDIA
TEST SERIES )

4 AIR

**YASH
JALUKA**
(ABHYAAS
TEST SERIES)

5 AIR

**MAMTA
YADAV**
(ALL INDIA
TEST SERIES )

6 AIR

**MEERA
K**
(ALL INDIA
TEST SERIES )

7 AIR

**PRAVEEN
KUMAR**
(ALL INDIA TEST SERIES )
ESSAY TEST, ABHYAAS , PDP)

8 AIR

**JIVANI KARTIK
NAGJIBHAI**
(GS FOUNDATION BATCH
CLASSROOM STUDENT)

9 AIR

**APALA
MISHRA**
(ABHYAAS
TEST SERIES)

10 AIR

**SATYAM
GANDHI**
(ALL INDIA TEST
SERIES , EASSY TEST)

**YOU CAN
BE
NEXT**

DELHI

**HEAD OFFICE** Apsara Arcade, 1/8-B, 1st Floor,
Near Gate 6, Karol Bagh Metro Station
**+91 8468022022, +91 9019066066**
**Mukherjee Nagar Centre**
635, Opp. Signature View Apartments,
Banda Bahadur Marg, Mukherjee Nagar

| JAIPUR | HYDERABAD | PUNE | AHMEDABAD | LUCKNOW | CHANDIGARH | GUWAHATI |
|---|---|---|---|---|---|---|
| 9001949244 | 9000104133 | 8007500096 | 9909447040 | 8468022022 | 8468022022 | 8468022022 |

/c/VisionIASdelhi /vision_ias /visionias_upsc /VisionIAS_UPSC