VISIONIAS
INSPIRING INNOVATION

# SECURITY

MAINS 365

Classroom Study Material 2022

( September 2021- to June 2022 )

8468022022, 9019066066 www.visionias.in

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

# SECURITY

## Table of Contents

**Previous Year Question**

A reference sheet of syllabus-wise segregated previous year questions from 2014-2021 (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,

- ⦿ Precision of content in good answer is no longer a dispensable luxury, but a simple necessity. And the preparation to write a precise answer starts well before one picks up a pen and starts to formulate the answer. A good understanding of the topic asked along-with a ready set of data and examples assists one in approaching the most difficult of the questions.
- ⦿ This is further assisted by a good presentation style, which depicts the information in an easy-to-understand manner.

**In this context, we made few changes to the Mains 365 documents last year, which included**

## Topic at glance:

which gave a comprehensive view of the topic, connecting the current and static aspects along-with providing necessary data and facts.

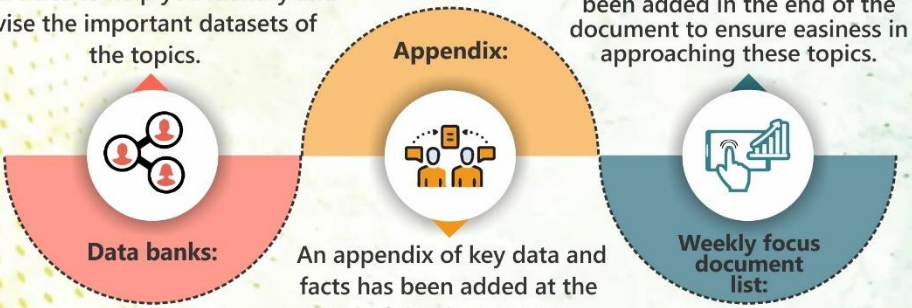
## Infographics:

Designed in a manner that they can be readily used in the answers

## Previous years questions:

A QR code linked syllabus wise segregated list of previous years questions was added.

**Along-with these, this year we have made few more additions to help you revise the topics and approach answers in a precise manner, these include:**



**Data banks:** have been designed and added in the articles to help you identify and revise the important datasets of the topics.

**Appendix:** An appendix of key data and facts has been added at the end of the document to facilitate quick revision.

**Weekly focus document list:** A QR code linked list of relevant Weekly focus documents has been added in the end of the document to ensure easiness in approaching these topics.

We hope that these additions will help you not only developing a comprehensive understanding of the topics but also provide the necessary inputs to write effective and well-presented answers.

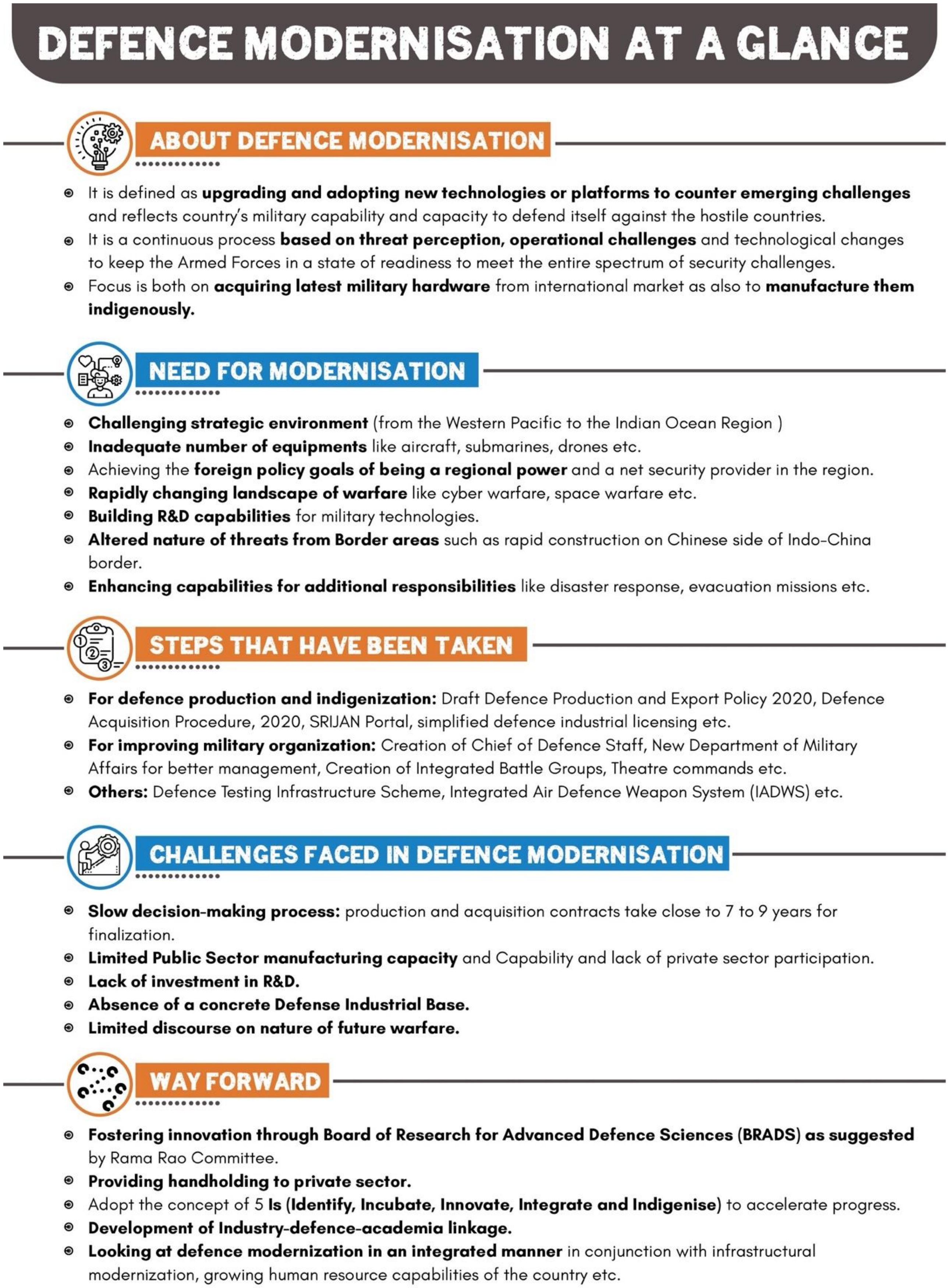
**Knowing is not enough: we must apply. Willing is not enough: we must do.**

-Johann Wolfgang von Goethe

All the best!
Team VisionIAS

# 1. DEFENCE

## 1.1. DEFENCE MODERNISATION



### DEFENCE MODERNISATION AT A GLANCE

#### ABOUT DEFENCE MODERNISATION

- It is defined as **upgrading and adopting new technologies or platforms to counter emerging challenges** and reflects country's military capability and capacity to defend itself against the hostile countries.
- It is a continuous process **based on threat perception, operational challenges** and technological changes to keep the Armed Forces in a state of readiness to meet the entire spectrum of security challenges.
- Focus is both on **acquiring latest military hardware** from international market as also to **manufacture them indigenously.**

#### NEED FOR MODERNISATION

- **Challenging strategic environment** (from the Western Pacific to the Indian Ocean Region )
- **Inadequate number of equipments** like aircraft, submarines, drones etc.
- Achieving the **foreign policy goals of being a regional power** and a net security provider in the region.
- **Rapidly changing landscape of warfare** like cyber warfare, space warfare etc.
- **Building R&D capabilities** for military technologies.
- **Altered nature of threats from Border areas** such as rapid construction on Chinese side of Indo-China border.
- **Enhancing capabilities for additional responsibilities** like disaster response, evacuation missions etc.

#### STEPS THAT HAVE BEEN TAKEN

- **For defence production and indigenization:** Draft Defence Production and Export Policy 2020, Defence Acquisition Procedure, 2020, SRIJAN Portal, simplified defence industrial licensing etc.
- **For improving military organization:** Creation of Chief of Defence Staff, New Department of Military Affairs for better management, Creation of Integrated Battle Groups, Theatre commands etc.
- **Others:** Defence Testing Infrastructure Scheme, Integrated Air Defence Weapon System (IADWS) etc.

#### CHALLENGES FACED IN DEFENCE MODERNISATION

- **Slow decision-making process:** production and acquisition contracts take close to 7 to 9 years for finalization.
- **Limited Public Sector manufacturing capacity** and Capability and lack of private sector participation.
- **Lack of investment in R&D.**
- **Absence of a concrete Defense Industrial Base.**
- **Limited discourse on nature of future warfare.**

#### WAY FORWARD

- **Fostering innovation through Board of Research for Advanced Defence Sciences (BRADS) as suggested** by Rama Rao Committee.
- **Providing handholding to private sector.**
- Adopt the concept of 5 **Is (Identify, Incubate, Innovate, Integrate and Indigenise)** to accelerate progress.
- **Development of Industry-defence-academia linkage.**
- **Looking at defence modernization in an integrated manner** in conjunction with infrastructural modernization, growing human resource capabilities of the country etc.

Mains 365 - Security

## 1.1.1. THEATRE COMMANDS

### Why in News?

Recently, for the first time Chief of Defence Staff (CDS) **publicly described the Indian military's deliberations** on reorganising itself into **Integrated Theatre Commands (ITCs)** stated that theatre commanders will report to CDS.

### More on News

- **Single-service commands** that currently exist would be **combined into just four geographical commands.**
  - **Western theatre command**: For the border against Pakistan.
  - **Northern theatre command**: For the border with China.
  - **Maritime command:** For Indian Ocean Region (IOR).
  - **Island command:** It is already functional, called the Andaman & Nicobar Command (ANC).
  - **Air space and cyber war** would be the 5th and 6th ITCs.

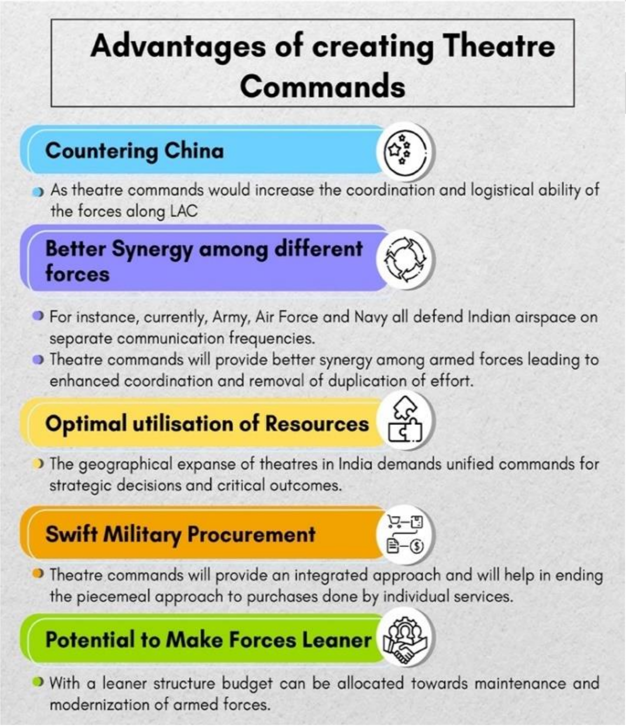
**Related Information**

**First National Maritime Security Coordinator appointed**

- Proposed after the 26/11 terror attacks (2008), the NMSC will be **part of the National Security Council Secretariat**, and will **report to National Security Adviser** (NSA).
  - NMSC has been a **long pending requirement since the Kargil Group of Ministers (GoM)** recommended it.
- **Role**
  - **Principal advisor to the government** on maritime security domain.
  - **To coordinate among the Indian Navy, the Coast Guard, security agencies** involved in coastal and maritime security and 13 coastal states and UTs.
    - ✓ At present, all these agencies **tend to work in silos with overlapping jurisdictions and are constantly at odds with each other.**

### What is a theatre command?

- Theaterisation or Theatre Command means **putting specific number of personnel from the three services**—army, navy and air force— **under a common commander** in a specified geographical territory.
- Idea of Theatre commands has been **proposed by both the Kargil review committee as well as D B Shekatkar committee.**



**Advantages of creating Theatre Commands**

**Countering China**

- As theatre commands would increase the coordination and logistical ability of the forces along LAC

**Better Synergy among different forces**

- For instance, currently, Army, Air Force and Navy all defend Indian airspace on separate communication frequencies.
- Theatre commands will provide better synergy among armed forces leading to enhanced coordination and removal of duplication of effort.

**Optimal utilisation of Resources**

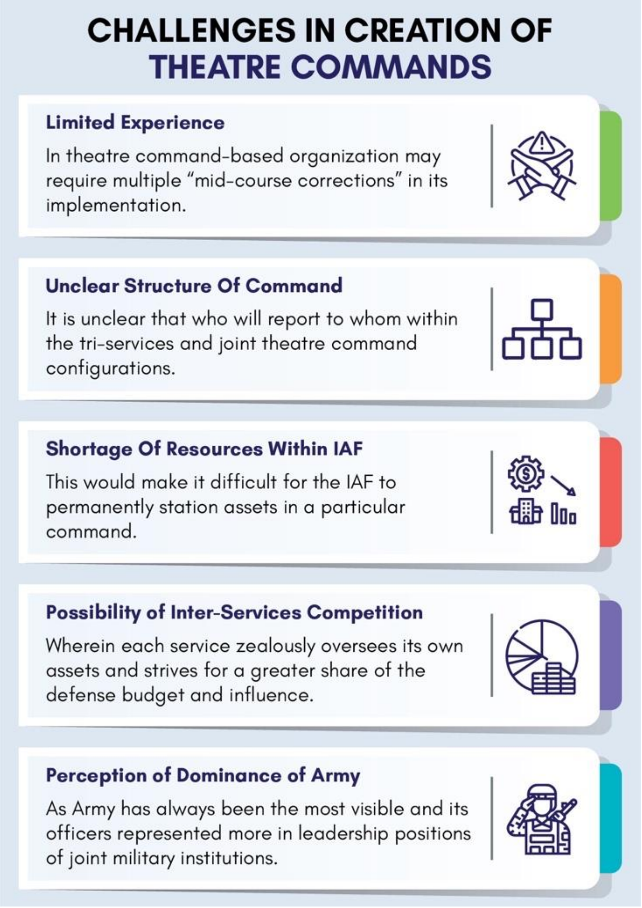
- The geographical expanse of theatres in India demands unified commands for strategic decisions and critical outcomes.

**Swift Military Procurement**

- Theatre commands will provide an integrated approach and will help in ending the piecemeal approach to purchases done by individual services.

**Potential to Make Forces Leaner**

- With a leaner structure budget can be allocated towards maintenance and modernization of armed forces.



**CHALLENGES IN CREATION OF THEATRE COMMANDS**

**Limited Experience**

In theatre command-based organization may require multiple "mid-course corrections" in its implementation.

**Unclear Structure Of Command**

It is unclear that who will report to whom within the tri-services and joint theatre command configurations.

**Shortage Of Resources Within IAF**

This would make it difficult for the IAF to permanently station assets in a particular command.

**Possibility of Inter-Services Competition**

Wherein each service zealously oversees its own assets and strives for a greater share of the defense budget and influence.

**Perception of Dominance of Army**

As Army has always been the most visible and its officers represented more in leadership positions of joint military institutions.

### Way Forward

Reorganization of the Military in the theatre command is not a solely institutional exercise, this change needs to be accompanied with other military reforms like-

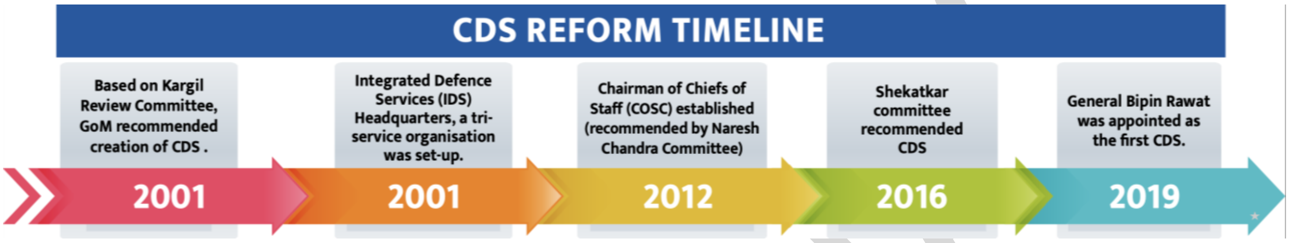
- Shifting to theatre command would require **development of military-industrial complex** to ensure self-sufficiency.
- Change in command structure would require **simultaneous changes in the Military-civilian decision making structure.**
- Government must **evaluate the efficacy of the current Integrated Defence Headquarters** including ANC.
- **Increasing Defense Spending** as India spends less than 2% of its GDP on Defense. This leads to a scenario of shortage in personnel, equipment and firepower.

## 1.1.2. CHIEF OF DEFENCE STAFF (CDS)

**Why in News?**

Ministry of Defense (MoD) issued a notification which broadens the scope of eligible officers for the post of the Chief of Defence Staff (CDS).

**About Chief of Defence Staff (CDS)**



CDS REFORM TIMELINE

2001 – Based on Kargil Review Committee, GoM recommended creation of CDS .

2001 – Integrated Defence Services (IDS) Headquarters, a tri-service organisation was set-up.

2012 – Chairman of Chiefs of Staff (COSC) established (recommended by Naresh Chandra Committee)

2016 – Shekatkar committee recommended CDS

2019 – General Bipin Rawat was appointed as the first CDS.

- CDS was created **to increase efficiency & coordination among the Armed Forces** and reduce duplication.
- **Aimed to**
  - **Achieve better results at all levels** through effective coordination between the Armed Forces and the Civil Services.
  - **Help facilitate inter-service integration** and better civilian-military coordination in the Nation's Higher Defence Organisation.
  - **Strengthen the process of Joint Planning, Operations and Procurement,** thereby making Armed Forces more effective and efficient.

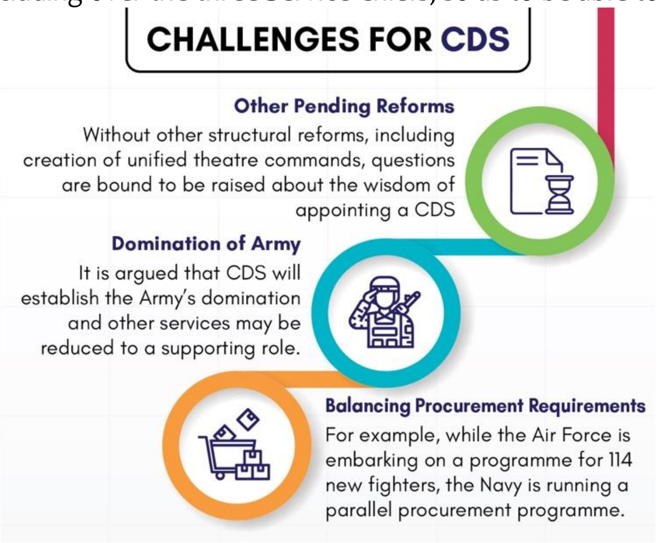
**Duties and functions of CDS**

- To **head the Department of Military Affairs (DMA)** in Ministry of Defence (MoD) and function as its secretary.
- To **act as the Principal Military Advisor to Defence Minister** on all Tri-Service matters.
- To **function as the Permanent Chairman of the Chiefs of Staff Committee** and to administer the Tri-Service organizations/agencies/commands.
- To be a **member of Defence Acquisition Council** and function as the Military Advisor to the Nuclear Command Authority.
- To ensure **optimal utilisation of infrastructure** and rationalise it through jointness among the Services.
- To **implement Five-Year Defence Capital Acquisition Plan and Two-Year roll-on Annual Acquisition Plans,** as a follow up of Integrated Capability Development Plan.

- CDS **does not exercise any military command,** including over the three Service Chiefs, so as to be able to provide impartial advice to the political leadership.

**Need of CDS**

- **Better advice to political executive:** CDS rises above inter-services rivalry and provide holistic advice on critical issues such as joint strategy and planning, weapons procurement, manpower allocation and joint operations.
  - **Can act as an arbitrator** when the Chiefs of Staff express divergent views on an issue, such as the use of military resources in the battlefield.
- **Integration of armed forces:** CDS is principally responsible for getting the armed forces better integrated rather than operating in silos.



CHALLENGES FOR CDS

**Other Pending Reforms**

Without other structural reforms, including creation of unified theatre commands, questions are bound to be raised about the wisdom of appointing a CDS

**Domination of Army**

It is argued that CDS will establish the Army's domination and other services may be reduced to a supporting role.

**Balancing Procurement Requirements**

For example, while the Air Force is embarking on a programme for 114 new fighters, the Navy is running a parallel procurement programme.

- **Constantly changing security dynamic:** Requires India's military needs to be efficient in combat and in averting adversaries, which is achievable only if the military is integrated.
- **Prioritizing procurement:** CDS can help meet country's military requirements in a manner that operational capabilities of forces are not compromised, and at the same time, needs are met with the available monetary resources.
- **Global similarity:** Many major countries like Italy, France, China, UK, USA etc. have created the post of CDS to bring more jointness and integration in their Armed Forces.

**Conclusion**

With the creation of CDS, India embarked upon a much-delayed process of integration of the armed forces and the defence establishment. CDS therefore must be supplemented by other structural reforms such as indigenous R&D, production of equipment, fostering innovation etc to improve the future readiness of the forces.

## 1.1.3. INTEGRATED BATTLE GROUPS (IBG)

**Why in news?**

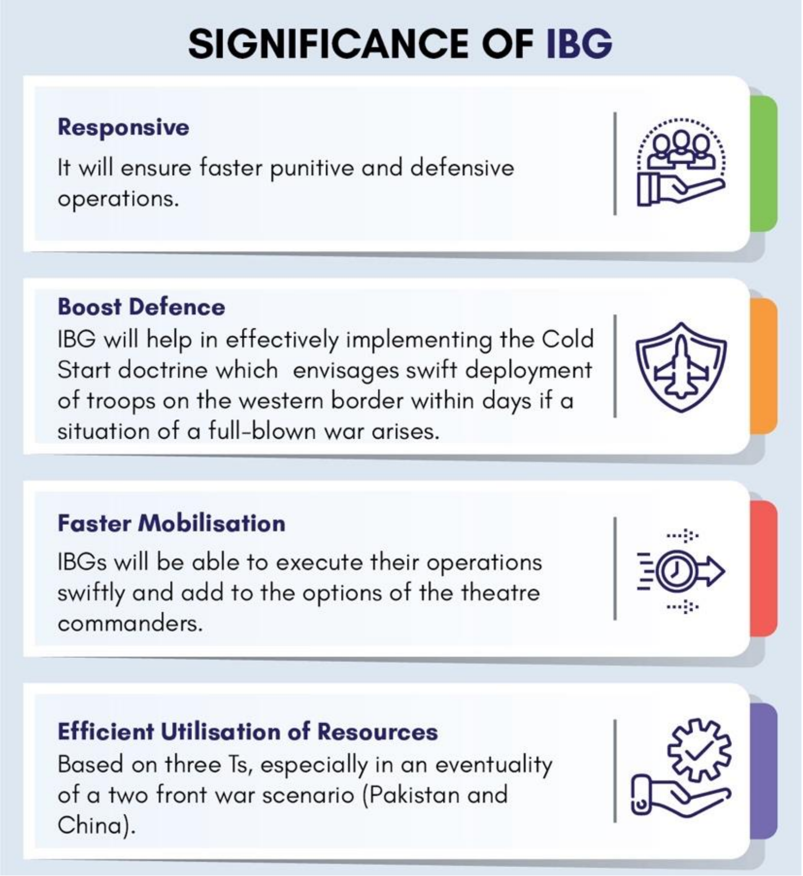
Recently, Army Chief said that IBG consultations are complete and are in the process of final compilation.

**About Proposed Integrated Battle Groups**

- IBGs are **brigade sized agile self-sufficient combat formations** which can swiftly launch strikes against adversary in case of hostilities.
  - Its objective is to **make the force more lethal and suitable to fight a modern war** with the support of technology.
  - Idea was tested in the plains and high altitudes in 2019.
- **Structure of IBG**
  - Each IBG would be tailor made **based on Threat, Terrain and Task** and resources will be allotted based on the **three Ts.** They **need to be light** so they will be low on logistics.
  - They will be able to **mobilise within 12-48 hours based on the location.**
  - Each IBG will likely be **headed by a Major General.**
  - IBGs involve the **integration of infantry, armoured tank regiments,** artillery, Unmanned Aerial Vehicles (UAVs), combat engineers and signals into one fighting unit.
  - IBGs will be **defensive and offensive.**

**Need for improving military organisations**

- **Two Front war:** Growing nexus on military and nuclear matters between Pakistan and China.
- **Enhance capabilities:** to achieve cross-spectrum (nuclear, conventional, counter sub-conventional) war-fighting capability to achieve a favourable outcome in case of a conflict.
- **Modernisation:** Army needs to be equipped with modern weapon systems to meet the needs and challenges of the future battlefields.
- **Improving Coordination:** among defence forces and intelligence agencies to boost intelligence gathering, sharing and surveillance and reconnaissance capabilities.
- **Multi-dimensional role:** to deal with external threats and also be prepared to assist in dealing with internal security threats.



SIGNIFICANCE OF IBG

**Responsive**
It will ensure faster punitive and defensive operations.

**Boost Defence**
IBG will help in effectively implementing the Cold Start doctrine which envisages swift deployment of troops on the western border within days if a situation of a full-blown war arises.

**Faster Mobilisation**
IBGs will be able to execute their operations swiftly and add to the options of the theatre commanders.

**Efficient Utilisation of Resources**
Based on three Ts, especially in an eventuality of a two front war scenario (Pakistan and China).

**Conclusion**

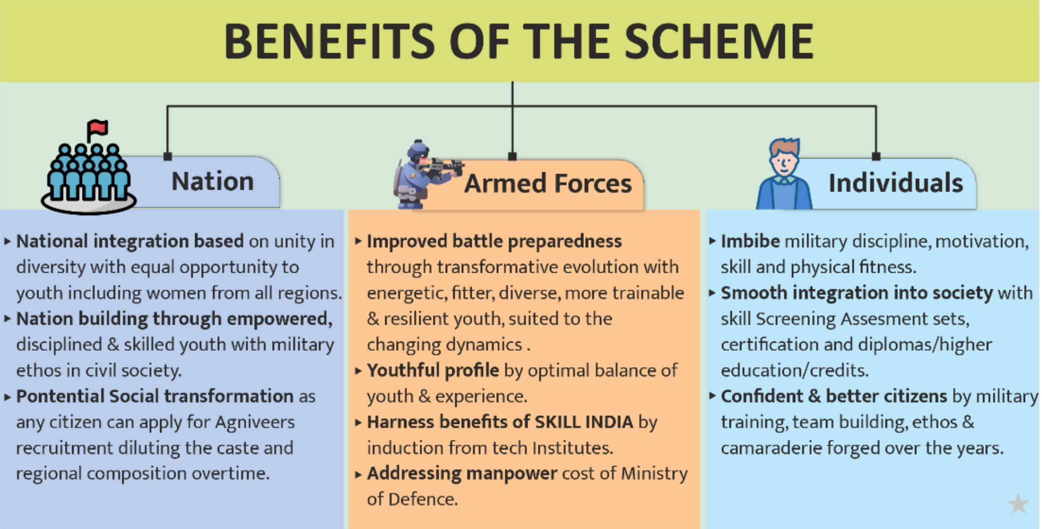
It is believed that, in 21st century, probability of full-scale wars to achieve decisive victories is likely to be very low. Future conflicts/wars were likely to be limited in time and space and dominated by high-end precision and lethal military technology.

In such wars, the requirement is of IBG type agile formations to gain the first–mover advantage.

## 1.1.4. AGNIPATH SCHEME

**Why in News?**

Union Cabinet approved Agnipath Scheme-a recruitment scheme for Indian youth to serve in the Armed Forces.



BENEFITS OF THE SCHEME

Nation

- **National integration based** on unity in diversity with equal opportunity to youth including women from all regions.
- **Nation building through empowered,** disciplined & skilled youth with military ethos in civil society.
- **Pontential Social transformation** as any citizen can apply for Agniveers recruitment diluting the caste and regional composition overtime.

Armed Forces

- **Improved battle preparedness** through transformative evolution with energetic, fitter, diverse, more trainable & resilient youth, suited to the changing dynamics .
- **Youthful profile** by optimal balance of youth & experience.
- **Harness benefits of SKILL INDIA** by induction from tech Institutes.
- **Addressing manpower** cost of Ministry of Defence.

Individuals

- **Imbibe** military discipline, motivation, skill and physical fitness.
- **Smooth integration into society** with skill Screening Assesment sets, certification and diplomas/higher education/credits.
- **Confident & better citizens** by military training, team building, ethos & camaraderie forged over the years.

**About Agnipath Scheme**

- It is a major defence policy reform to **usher in a new era in the Human Resource policy** of the three Services.
    - Idea of a **short-term recruitment model or 'Tour of Duty' (ToD) was first mooted around two years back** for the selection of officers and jawans, for a limited number of vacancies.
- **Youth (from 17.5 years to 23 age group) selected under this scheme will be known as Agniveers** who will be enrolled for a period of **four years**. They would form **a distinct rank in the Armed Forces**, different from any other existing ranks.
- **Upon the completion of four years of service,** Agniveers will be offered an **opportunity to apply for permanent enrolment** in the Armed Forces.
    - **Up to 25% of each specific batch will be enrolled in regular cadre** based on objective criteria including performance during their four-year engagement period.

**Global practices**

A careful analysis of methodology of induction, retention, and release of armed forces personnel in various developed countries shows similar kind of reforms in recruitment. For ex:

- **Russian military is a hybrid format** combining a traditional cadre-and-reserve conscript system (includes one year of training and one year of service) and a contract-professional system.
- In **Israel period of active-duty conscript is 32 months for men and 24 months for women,** followed by a decades-long period of compulsory reserve duty.
- For **French soldiers there are two types of enlistment:** 1 year contract or 3-5 years contract (both renewable).

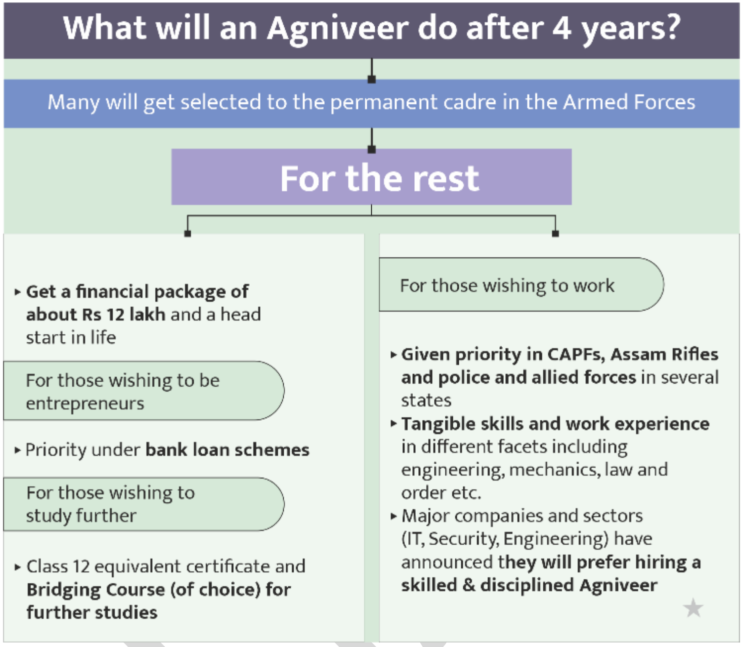
**Concerns related to scheme**

- **Building cohesion:** Time period for Agnipath is too short to build cohesion as it is built over a long period of living, training and experiencing rigours of field/operational/counter-insurgency tenures together.
- **Might not attract best candidates:** as they are likely to apply for more permanent avenues like police or paramilitary forces first.
- **Unfair to the potential recruit:** at the expiry of four years when he's still in his 20s and without the skillsets or credentials required to thrive in the civilian/corporate world.
- **Less training time:** It reportedly takes two to three years to train a member of the army, but as a part of the Agnipath scheme, soldiers will only be trained for six months.
    - Defence analysts have allegedly pointed out that the Russian soldiers who were trained for a limited amount of time before they went to war in Ukraine have performed disastrously.

- **Potentially militarize the society:** With their ambitions of serving in the military for a full 15 years, frustrated and unemployed, the demobilised Agniveers could fall prey to the lure of crime syndicates and radical political outfits.
- **Disturbing the regional balance:** With the scheme calling for recruitment on an all-India basis, rather than by state allotments, army's ranks could well become northern states heavy, disturbing regional balance within the military.

**Way forward**

- **Scheme needs to be linked to other manpower management related reforms.**
- **Educational qualification can be raised** to 10+2 and a more stringent all-India merit-driven entrance examination with psychological tests must be introduced for a shift towards a more tech-savvy armed forces.
- Due care must be taken to ensure that the Agnipath scheme **does not upset the regimental ethos of the Indian Army.**
- Reduced training period will have to be offset by **focused training and employment of other innovative methods.** Also, Army leadership will have to employ innovative devices to inculcate loyalty and camaraderie in quick time.
- **Incentivise this new scheme.** For instance, in the US the short-term duty soldiers undergo education at government expense.



What will an Agniveer do after 4 years?

Many will get selected to the permanent cadre in the Armed Forces

For the rest

- **Get a financial package of about Rs 12 lakh** and a head start in life

For those wishing to be entrepreneurs

- Priority under **bank loan schemes**

For those wishing to study further

- Class 12 equivalent certificate and **Bridging Course (of choice) for further studies**

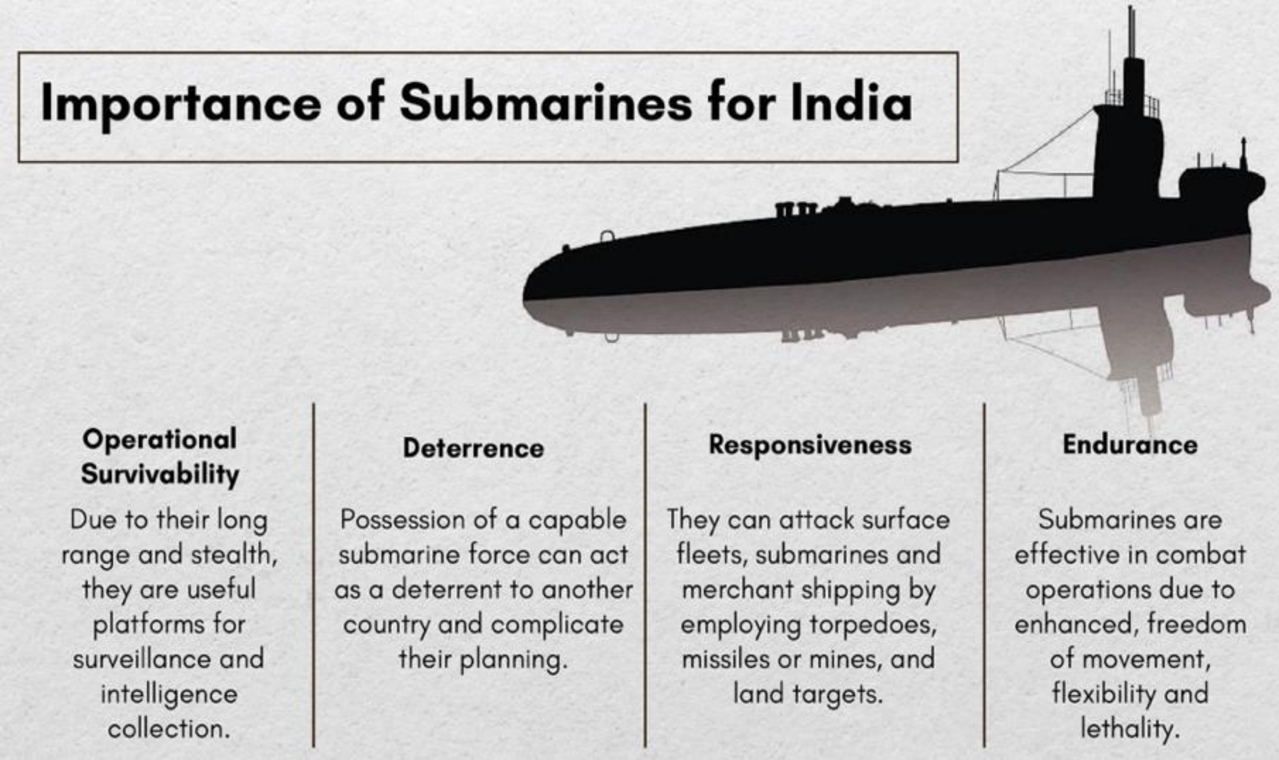
For those wishing to work

- **Given priority in CAPFs, Assam Rifles and police and allied forces** in several states
- **Tangible skills and work experience** in different facets including engineering, mechanics, law and order etc.
- Major companies and sectors (IT, Security, Engineering) have announced **they will prefer hiring a skilled & disciplined Agniveer**

## 1.1.5. SUBMARINE IN INDIA

**Why in news?**

Recently, France's Naval Group has **declined the bid for Navy's P-75 India (P-75I) project** as it does not use Air-Independent Propulsion (AIP) system.



Importance of Submarines for India

**Operational Survivability**

Due to their long range and stealth, they are useful platforms for surveillance and intelligence collection.

**Deterrence**

Possession of a capable submarine force can act as a deterrent to another country and complicate their planning.

**Responsiveness**

They can attack surface fleets, submarines and merchant shipping by employing torpedoes, missiles or mines, and land targets.

**Endurance**

Submarines are effective in combat operations due to enhanced, freedom of movement, flexibility and lethality.

### About P-75I and P 75

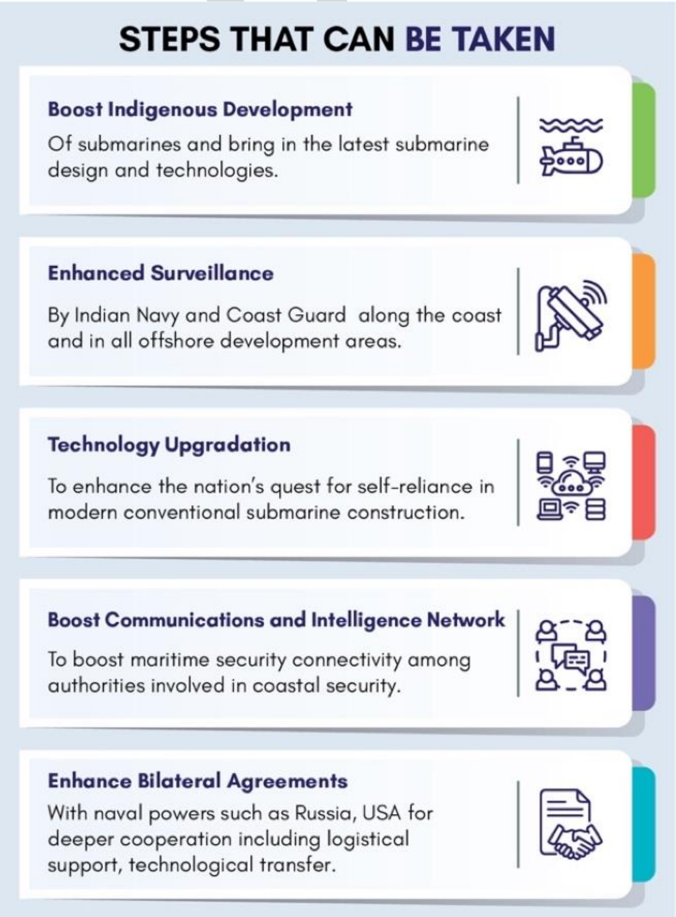
- P-75I, succeeds the P75, is **part of 30-year submarine building plan that ends in 2030.** This will be the **first under the strategic partnership (SP) model,** promulgated by the Defence Acquisition Council (DAC) in 2017.
    - It will help to **reduce dependence on imports** and gradually **ensure greater self-reliance and dependability of supplies** from indigenous source.
- **P-75 was signed in 2005** and **first Kalvari Class (Scorpene Class) submarine** under the project was commissioned in 2017.
    - It includes construction of six submarines of **Scorpene (diesel-electric) design.**

### Classification of Submarines

| Submersible Ship Ballistic Nuclear (SSBNs) | Nuclear-Powered attack submarines (SSNs) | Diesel-electric attack submarines (SSKs) |
|---|---|---|
| • Often referred to as **"boomers,"** serve as an **undetectable launch platform for intercontinental missiles.**<br>• They are **designed specifically for stealth** and **the precise delivery** of nuclear warheads.<br>• India has **one nuclear ballistic submarine i.e. INS Arihant (S2).** | • It is **armed with non-nuclear weapons.**<br>• Provide Navy **capacity to carry out intelligence, surveillance, and covert deployment** of Special Operations Forces.<br>• Only **6 countries** currently have **nuclear-powered submarines- UK, US, China, Russia, India and France.** | • They have **two or more diesel engines.**<br>• The battery capacity can **constrain the amount of time a diesel sub can stay underwater,** leading to frequent resurfacing and thus can be **easily detected.**<br>• India has **15 conventional diesel-electric submarines.** |

### Issues with India's naval build-up

- **Delays and Aged Fleet:** India's current conventional submarine fleet is severely aged. After INS Kalvari, inducted recently, the next youngest conventional submarine with the Navy is 17 years old.
- **Contractual Obligations:** The Akula class submarine, INS Chakra, on lease from Russia, is only for training Indian sailors and is not permitted to carry nuclear missiles or be deployed on operational roles.
- **Limited endurance:** For instance, INS Arihant's nuclear reactor has a short refueling cycle and therefore a limited endurance capacity.
- **Lackadaisical Development:** Slow development of AIP system by DRDO has led to a significant delay for the Indian Navy's submarine plans.
- **Lack of Infrastructure:** Shortfalls in essentials capacities such as advanced towed array sonars (ATAS) to detect enemy submarines, heavyweight torpedoes to neutralize them etc.
- **Funding:** Figures from FY2017-2018 indicate that India spends only 15 percent of its total military expenditure on its navy, far lower than its peers in the Quad.



STEPS THAT CAN BE TAKEN

**Boost Indigenous Development**
Of submarines and bring in the latest submarine design and technologies.

**Enhanced Surveillance**
By Indian Navy and Coast Guard along the coast and in all offshore development areas.

**Technology Upgradation**
To enhance the nation's quest for self-reliance in modern conventional submarine construction.

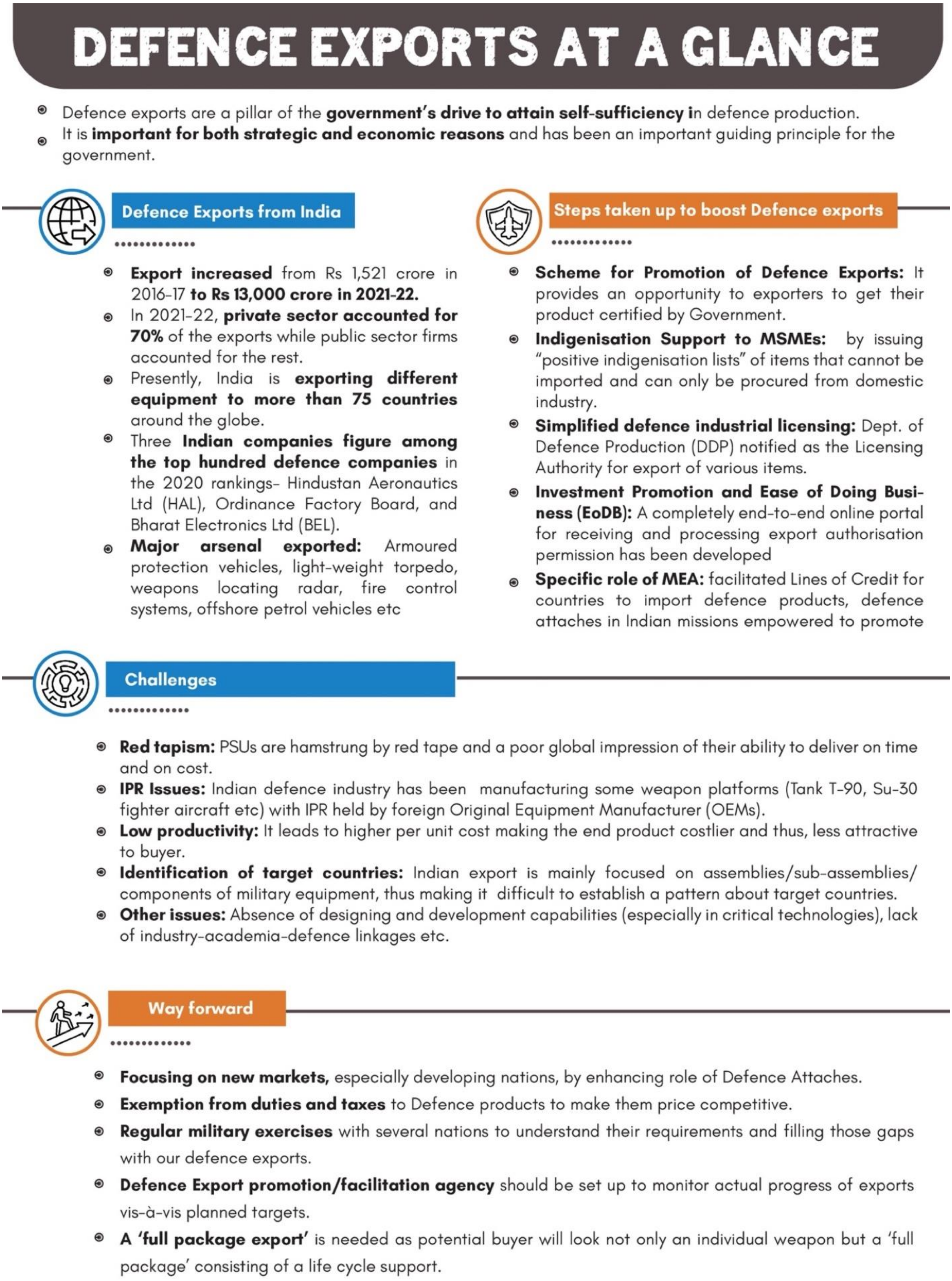
**Boost Communications and Intelligence Network**
To boost maritime security connectivity among authorities involved in coastal security.

**Enhance Bilateral Agreements**
With naval powers such as Russia, USA for deeper cooperation including logistical support, technological transfer.

### Conclusion

As most of India's submarines are over 25 years old, there is a need to fast track submarine building plan in India for our own maritime security and also to counter Chinese presence in the Indian Ocean in the coming years.

## 1.2. DEFENCE EXPORTS



# DEFENCE EXPORTS AT A GLANCE

- Defence exports are a pillar of the **government's drive to attain self-sufficiency i**n defence production.
- It is **important for both strategic and economic reasons** and has been an important guiding principle for the government.

### Defence Exports from India

- **Export increased** from Rs 1,521 crore in 2016-17 **to Rs 13,000 crore in 2021-22.**
- In 2021-22, **private sector accounted for 70%** of the exports while public sector firms accounted for the rest.
- Presently, India is **exporting different equipment to more than 75 countries** around the globe.
- Three **Indian companies figure among the top hundred defence companies** in the 2020 rankings- Hindustan Aeronautics Ltd (HAL), Ordinance Factory Board, and Bharat Electronics Ltd (BEL).
- **Major arsenal exported:** Armoured protection vehicles, light-weight torpedo, weapons locating radar, fire control systems, offshore petrol vehicles etc

### Steps taken up to boost Defence exports

- **Scheme for Promotion of Defence Exports:** It provides an opportunity to exporters to get their product certified by Government.
- **Indigenisation Support to MSMEs:** by issuing "positive indigenisation lists" of items that cannot be imported and can only be procured from domestic industry.
- **Simplified defence industrial licensing:** Dept. of Defence Production (DDP) notified as the Licensing Authority for export of various items.
- **Investment Promotion and Ease of Doing Business (EoDB):** A completely end-to-end online portal for receiving and processing export authorisation permission has been developed
- **Specific role of MEA:** facilitated Lines of Credit for countries to import defence products, defence attaches in Indian missions empowered to promote

### Challenges

- **Red tapism:** PSUs are hamstrung by red tape and a poor global impression of their ability to deliver on time and on cost.
- **IPR Issues:** Indian defence industry has been manufacturing some weapon platforms (Tank T-90, Su-30 fighter aircraft etc) with IPR held by foreign Original Equipment Manufacturer (OEMs).
- **Low productivity:** It leads to higher per unit cost making the end product costlier and thus, less attractive to buyer.
- **Identification of target countries:** Indian export is mainly focused on assemblies/sub-assemblies/ components of military equipment, thus making it difficult to establish a pattern about target countries.
- **Other issues:** Absence of designing and development capabilities (especially in critical technologies), lack of industry-academia-defence linkages etc.

### Way forward

- **Focusing on new markets,** especially developing nations, by enhancing role of Defence Attaches.
- **Exemption from duties and taxes** to Defence products to make them price competitive.
- **Regular military exercises** with several nations to understand their requirements and filling those gaps with our defence exports.
- **Defence Export promotion/facilitation agency** should be set up to monitor actual progress of exports vis-à-vis planned targets.
- **A 'full package export'** is needed as potential buyer will look not only an individual weapon but a 'full package' consisting of a life cycle support.

### 1.2.1. BRAHMOS

**Why in News?**

Recently, Philippines signed a $375 million deal for BrahMos supersonic cruise missiles.

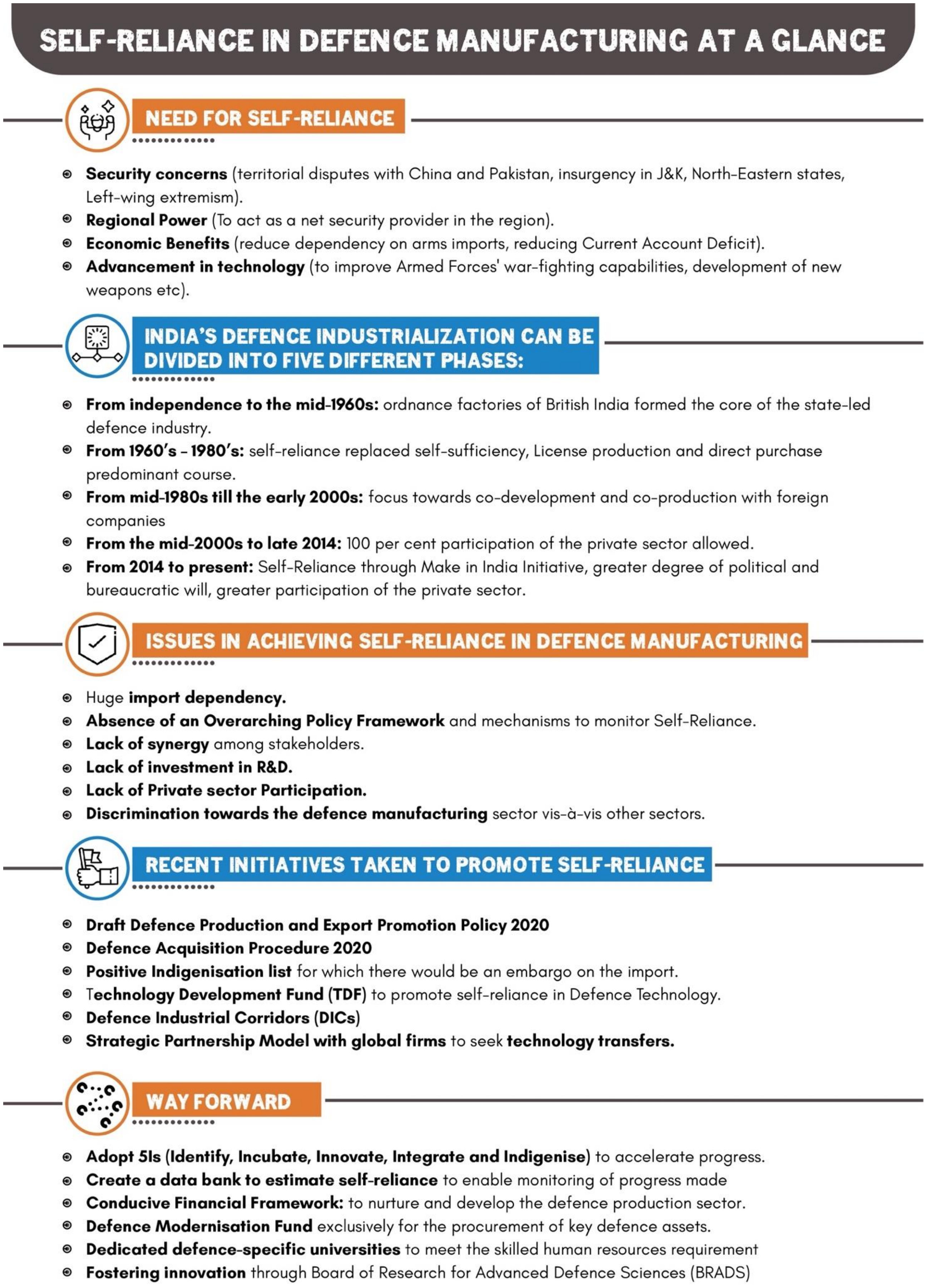
**Other similar missile systems**

- **Chinese HD-1 supersonic missile**
  - Missile platform can be adapted to aircraft and ships as well as the basic ground-based vehicle version.
  - HD-1 needs less fuel than its competitors, rendering the lighter missile able to fly faster and farther.
- **Tomahawk (used by U.S and its allies)** is a long-range, all-weather, subsonic cruise missile that launches from ships and submarines and can strike targets precisely from 1,000 miles away.
- **Israel's Sea Breaker,** the 5th generation long range, autonomous, precision-guided missile system, is meant to hit high-value maritime and land targets
- **P-800 Oniks/Yakhont** is a Russian supersonic anti-ship cruise missiles that has an effective guidance system and is a fire-and-forget missile.

**About BrahMos**

- **BrahMos is a universal long range supersonic cruise missile** system that can be launched from land, sea and air against surface and sea-based targets.
  - BrahMos is a **joint collaboration** between India (DRDO) and Russia (NPO Mashinostoyenia).
  - Name represents Brahmaputra and Moskva rivers.
- **It is a two-stage missile** with a solid propellant booster engine as first stage and liquid ramjet as second stage.
  - It operates at **fire and forget principle.**
- The range of the missile **was originally capped at 290 km** as per obligations of the Missile Technology Control Regime (MTCR).
  - **Following India's entry in MTCR in 2016,** it was decided to extend the range to 450 km and to 600 km at a later stage.

## 1.3. SELF-RELIANCE IN DEFENCE MANUFACTURING



## SELF-RELIANCE IN DEFENCE MANUFACTURING AT A GLANCE

### NEED FOR SELF-RELIANCE

- **Security concerns** (territorial disputes with China and Pakistan, insurgency in J&K, North-Eastern states, Left-wing extremism).
- **Regional Power** (To act as a net security provider in the region).
- **Economic Benefits** (reduce dependency on arms imports, reducing Current Account Deficit).
- **Advancement in technology** (to improve Armed Forces' war-fighting capabilities, development of new weapons etc).

### INDIA'S DEFENCE INDUSTRIALIZATION CAN BE DIVIDED INTO FIVE DIFFERENT PHASES:

- **From independence to the mid-1960s:** ordnance factories of British India formed the core of the state-led defence industry.
- **From 1960's – 1980's:** self-reliance replaced self-sufficiency, License production and direct purchase predominant course.
- **From mid-1980s till the early 2000s:** focus towards co-development and co-production with foreign companies
- **From the mid-2000s to late 2014:** 100 per cent participation of the private sector allowed.
- **From 2014 to present:** Self-Reliance through Make in India Initiative, greater degree of political and bureaucratic will, greater participation of the private sector.

### ISSUES IN ACHIEVING SELF-RELIANCE IN DEFENCE MANUFACTURING

- Huge **import dependency.**
- **Absence of an Overarching Policy Framework** and mechanisms to monitor Self-Reliance.
- **Lack of synergy** among stakeholders.
- **Lack of investment in R&D.**
- **Lack of Private sector Participation.**
- **Discrimination towards the defence manufacturing** sector vis-à-vis other sectors.

### RECENT INITIATIVES TAKEN TO PROMOTE SELF-RELIANCE

- **Draft Defence Production and Export Promotion Policy 2020**
- **Defence Acquisition Procedure 2020**
- **Positive Indigenisation list** for which there would be an embargo on the import.
- T**echnology Development Fund (TDF)** to promote self-reliance in Defence Technology.
- **Defence Industrial Corridors (DICs)**
- **Strategic Partnership Model with global firms** to seek **technology transfers.**

### WAY FORWARD

- **Adopt 5Is (Identify, Incubate, Innovate, Integrate and Indigenise)** to accelerate progress.
- **Create a data bank to estimate self-reliance** to enable monitoring of progress made
- **Conducive Financial Framework:** to nurture and develop the defence production sector.
- **Defence Modernisation Fund** exclusively for the procurement of key defence assets.
- **Dedicated defence-specific universities** to meet the skilled human resources requirement
- **Fostering innovation** through Board of Research for Advanced Defence Sciences (BRADS)

## 1.3.1. TECHNOLOGY DEVELOPMENT FUND (TDF)

**Why in news?**

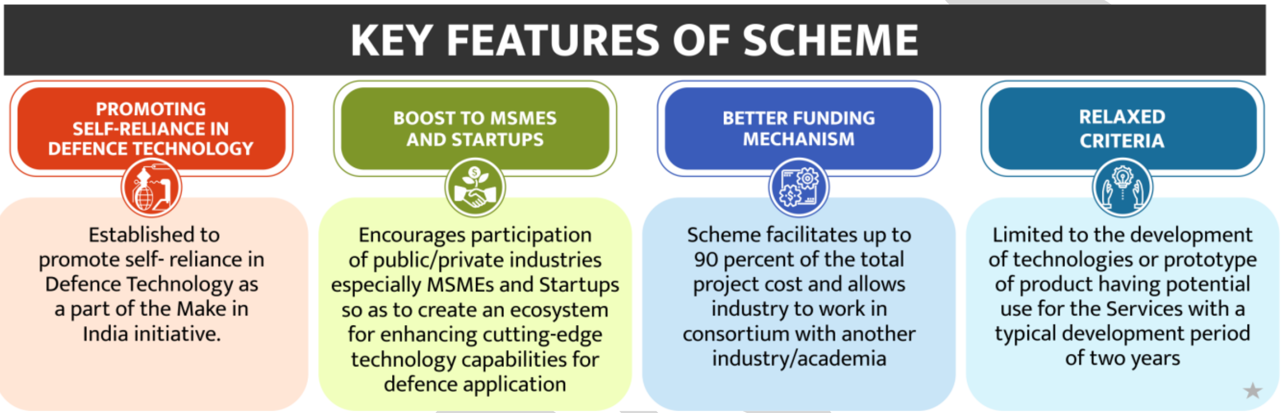
Recently, limit of funding of innovative defense projects under Technology Development Fund (TDF) has been raised to Rs 50 crore per project, from the present limit of Rs 10 crore.

**More on News**

- To facilitate increased funding for innovative TDF products, **Union Budget for 2022-23 has reserved 25 per cent of the defence R&D budget** for private industry, start-ups and academia.
- Enhanced funding **will further boost the vision of 'Aatmanirbharta'** (self-reliance) in defence.

**About Technology Development Fund (TDF) scheme**

- Executed by the Defence Research and Development Organisation (DRDO), TDF aims **to create an ecosystem for promoting self-reliance** by building indigenous state-of-the-art systems for defence application.



KEY FEATURES OF SCHEME

PROMOTING SELF-RELIANCE IN DEFENCE TECHNOLOGY

Established to promote self- reliance in Defence Technology as a part of the Make in India initiative.

BOOST TO MSMES AND STARTUPS

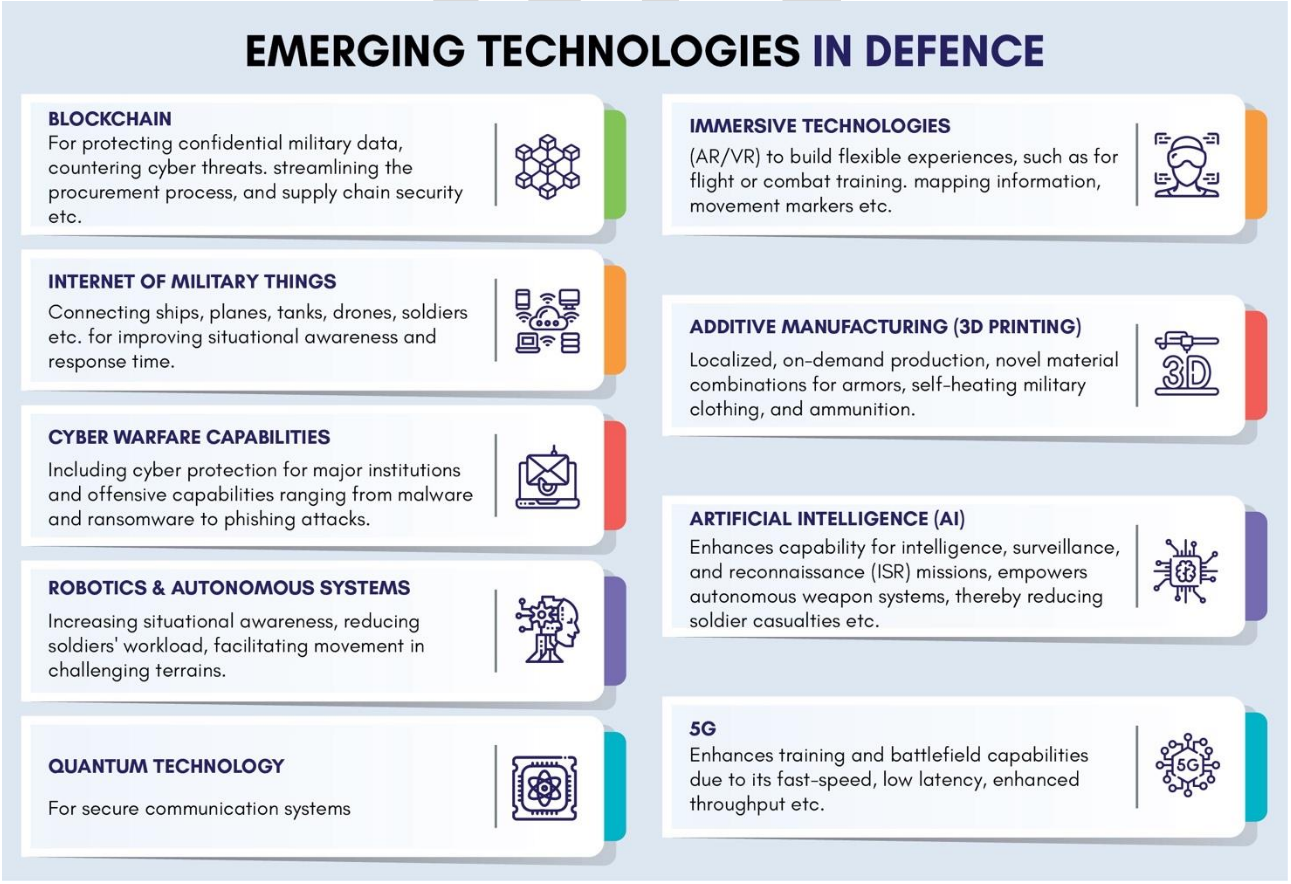
Encourages participation of public/private industries especially MSMEs and Startups so as to create an ecosystem for enhancing cutting-edge technology capabilities for defence application

BETTER FUNDING MECHANISM

Scheme facilitates up to 90 percent of the total project cost and allows industry to work in consortium with another industry/academia

RELAXED CRITERIA

Limited to the development of technologies or prototype of product having potential use for the Services with a typical development period of two years



EMERGING TECHNOLOGIES IN DEFENCE

BLOCKCHAIN

For protecting confidential military data, countering cyber threats. streamlining the procurement process, and supply chain security etc.

INTERNET OF MILITARY THINGS

Connecting ships, planes, tanks, drones, soldiers etc. for improving situational awareness and response time.

CYBER WARFARE CAPABILITIES

Including cyber protection for major institutions and offensive capabilities ranging from malware and ransomware to phishing attacks.

ROBOTICS & AUTONOMOUS SYSTEMS

Increasing situational awareness, reducing soldiers' workload, facilitating movement in challenging terrains.

QUANTUM TECHNOLOGY

For secure communication systems

IMMERSIVE TECHNOLOGIES

(AR/VR) to build flexible experiences, such as for flight or combat training. mapping information, movement markers etc.

ADDITIVE MANUFACTURING (3D PRINTING)

Localized, on-demand production, novel material combinations for armors, self-heating military clothing, and ammunition.

ARTIFICIAL INTELLIGENCE (AI)

Enhances capability for intelligence, surveillance, and reconnaissance (ISR) missions, empowers autonomous weapon systems, thereby reducing soldier casualties etc.

5G

Enhances training and battlefield capabilities due to its fast-speed, low latency, enhanced throughput etc.

## 1.4. MILITARY LOGISTICS AGREEMENTS

### Why in News?

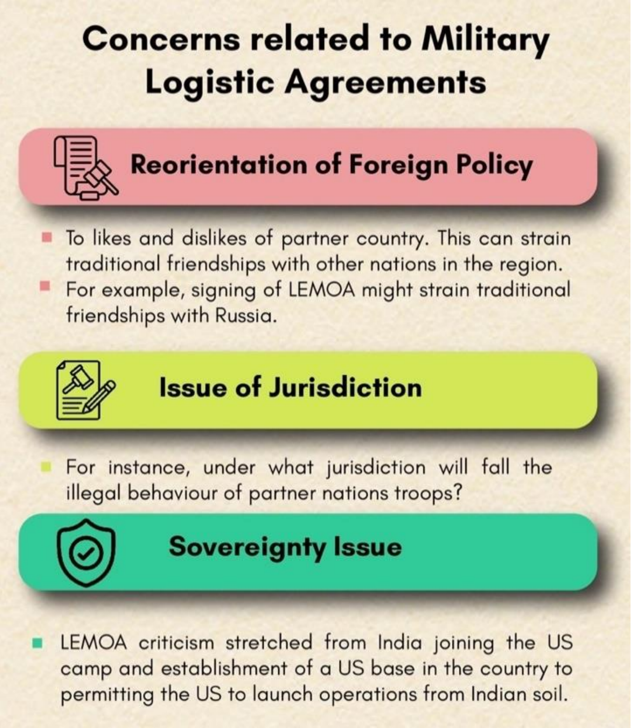
India and Vietnam have signed a **logistics support pact to allow militaries** of both sides to **use each other's bases for repair and replenishment of supplies**

### What are Military Logistics agreements?

- These are merely administrative arrangements that would facilitate replenishment of fuel, rations, and spare parts, as well as berthing and maintenance for each other's warships, military aircraft, and troops during port visits and joint exercises, on a reciprocal basis, essentially simplifying the process of extending logistical support to one other.

**India's military logistics agreements**

- India has such agreements with Australia, Japan, US – the **Quad countries – as well as with France, Singapore and South Korea.**
- Also, India is currently in the process of **finalizing such an agreement with U.K. and Russia** and in talks with other **partners.**



**Concerns related to Military Logistic Agreements**

**Reorientation of Foreign Policy**

- To likes and dislikes of partner country. This can strain traditional friendships with other nations in the region.
- For example, signing of LEMOA might strain traditional friendships with Russia.

**Issue of Jurisdiction**

- For instance, under what jurisdiction will fall the illegal behaviour of partner nations troops?

**Sovereignty Issue**

- LEMOA criticism stretched from India joining the US camp and establishment of a US base in the country to permitting the US to launch operations from Indian soil.

### Benefits of Military Logistics agreements

- **Expanding India's Military reach:** especially maritime outreach and influence in various regions that are strategically important to India. For example:
  - Reciprocal Exchange of Logistics Agreement (RELOS) with Russia gives India access to Russian facilities in the Arctic region.
  - Logistics Exchange Memorandum of Agreement (LEMOA) provides India access to U.S. military facilities in Djibouti, Diego Garcia, Guam, and Subic Bay.
- **Saves time and cost:** of the lengthy bookkeeping exercises that the militaries have to otherwise do with each visit.
- **Enhanced cooperation and greater inter-operability between Nations:** during activities such as peacekeeping operations, humanitarian assistance and disaster relief (HADR) etc.
- **Strategic importance:** It permits a country to project power away from its borders in international waters.
- **Edge to Indian Navy:** These agreements have enhanced operational turnaround and strengthened interoperability among Indian and partner navies on the high seas.

### Conclusion

India shied away from concluding military logistic agreements for more than a decade. But changing geopolitical situation and an assertive China has facilitated India's embrace of like-minded partners across the Indo-Pacific, including through logistics agreements.

# 2. DATA PROTECTION

## 2.1. DATA PRIVACY AND INNOVATION

### DATA PRIVACY AND INNOVATION AT A GLANCE

**Data** is representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means.

**Personal data:** Data relating to a natural person that directly or indirectly identifies that individual.

**Non-personal data:** Data that is completely unrelated to an identifiable natural person.

**Data Privacy has 3 key elements:**

- Control over personal data.
- Procedures for proper handling, processing, collecting, and sharing of personal data.
- Compliance with data protection laws

#### Implications of data driven innovation on the privacy of users

- **Data breaches:** Can have adverse effects on privacy of users including public humiliation, identity theft, financial fraud, harassment, stalking etc.
- **Profiling of individuals:** Can be used for unequal treatment or discrimination.
- **Erosion of individual autonomy:** Can place direct or indirect restriction on an individual's speech, movement and can influence opinions, jeopardizing **autonomous thinking.**
- **Lack of real alternatives:** Restricts the choices of users to safeguard their own privacy.
- **Potential for data misuse:** Users have little control over data usage and practices.

#### Benefits of privacy considerations in innovation

- **Enabling effective and high-quality data collection:** by encouraging voluntary sharing of data.
- **Creating a niche market:** in the field of Privacy Enhancing Technologies.
- **Generating consumer demand through trust**
- **Facilitating creativity:** by creating a sense of security against issues like surveillance and profiling.
- **Enhancing competition:** by establishing a level playing field vis-à-vis access to data

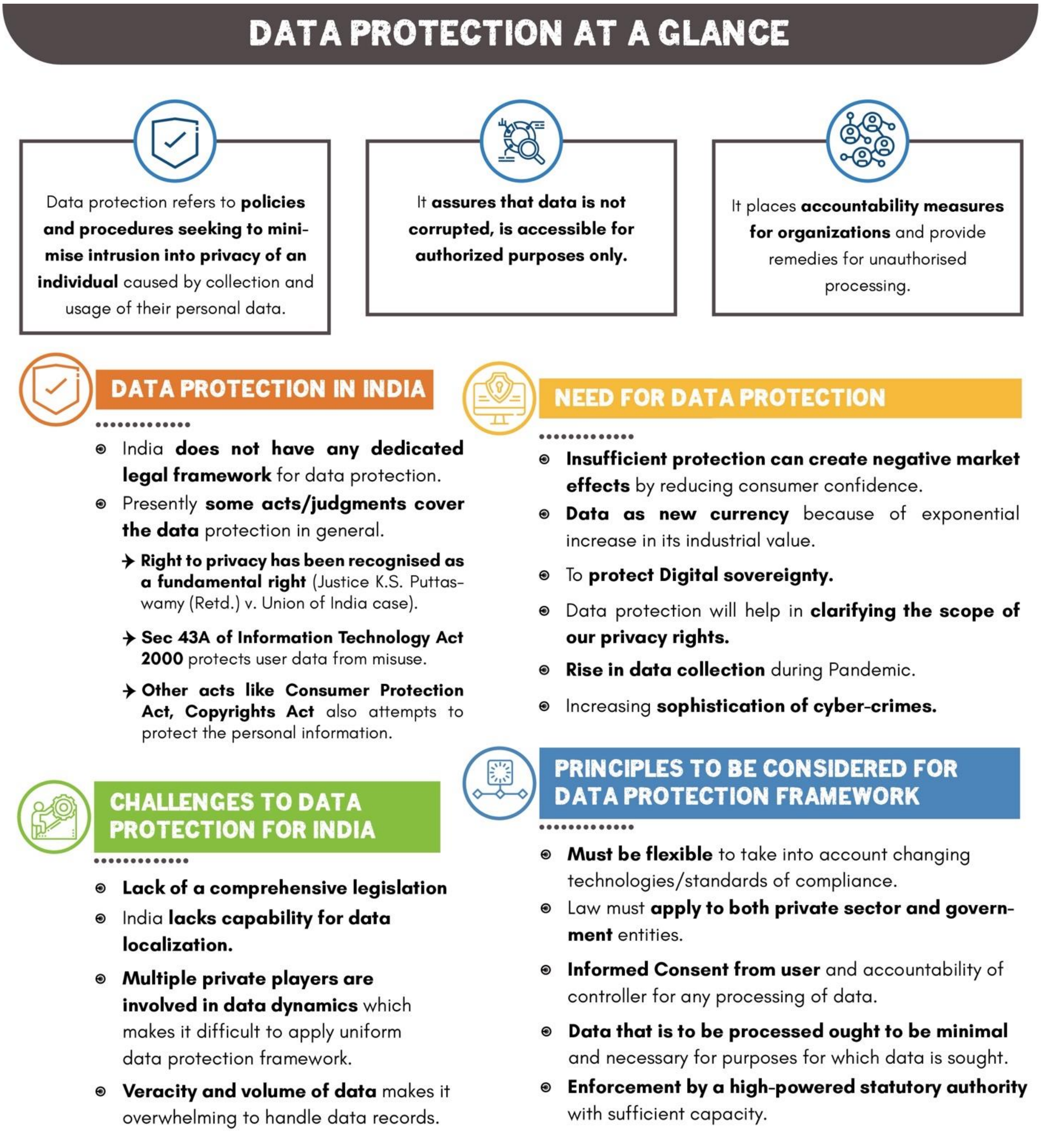
#### Challenges with inclusion of privacy considerations in innovation

- **Escalation of costs:** to maintain full compliance with restrictive privacy.
- **Business Uncertainty:** due uncertain regulatory environment surrounding technology and privacy laws.
- **Precautionary principle** (that emphasizes caution, pausing and review before leaping into new innovations) may discourage entrepreneurial ideas and start up culture.
- **Creation of oligopolistic market structures:** Disproportionate damage to small companies, start-ups etc. due to reasons such as **Technical and financial challenges in complying with regulations, creation of walled gardens on the Internet and data monopoly.**
- **Hindered information flow**

#### Way Forward: Promoting data privacy while protecting innovation

- **Anonymization of personal data sets:** through techniques like Pseudonymization/ De-identification, Anonymization and Transforming information into statistical data.
- **Collecting only relevant data and making optimal use of it**
- **Revamping regulatory regimes**
- **Promoting privacy-respecting technological innovations**
- **Encouraging privacy by design** (data handling practices that ensures compliance with the law by minimizing or eliminating adverse impacts on privacy)
- **Creating universally-available datasets** to enhance access to data for startups
- **Data empowerment:** Process where people, on their own or with the help of intermediaries, take control or gain the power to take control of their data

## 2.2. DATA PROTECTION IN INDIA



# DATA PROTECTION AT A GLANCE

Data protection refers to **policies and procedures seeking to minimise intrusion into privacy of an individual** caused by collection and usage of their personal data.

It **assures that data is not corrupted, is accessible for authorized purposes only.**

It places **accountability measures for organizations** and provide remedies for unauthorised processing.

### DATA PROTECTION IN INDIA

- India **does not have any dedicated legal framework** for data protection.
- Presently **some acts/judgments cover the data** protection in general.
  - **Right to privacy has been recognised as a fundamental right** (Justice K.S. Puttaswamy (Retd.) v. Union of India case).
  - **Sec 43A of Information Technology Act 2000** protects user data from misuse.
  - **Other acts like Consumer Protection Act, Copyrights Act** also attempts to protect the personal information.

### CHALLENGES TO DATA PROTECTION FOR INDIA

- **Lack of a comprehensive legislation**
- India **lacks capability for data localization.**
- **Multiple private players are involved in data dynamics** which makes it difficult to apply uniform data protection framework.
- **Veracity and volume of data** makes it overwhelming to handle data records.

### NEED FOR DATA PROTECTION

- **Insufficient protection can create negative market effects** by reducing consumer confidence.
- **Data as new currency** because of exponential increase in its industrial value.
- To **protect Digital sovereignty.**
- Data protection will help in **clarifying the scope of our privacy rights.**
- **Rise in data collection** during Pandemic.
- Increasing **sophistication of cyber-crimes.**

### PRINCIPLES TO BE CONSIDERED FOR DATA PROTECTION FRAMEWORK

- **Must be flexible** to take into account changing technologies/standards of compliance.
- Law must **apply to both private sector and government** entities.
- **Informed Consent from user** and accountability of controller for any processing of data.
- **Data that is to be processed ought to be minimal** and necessary for purposes for which data is sought.
- **Enforcement by a high-powered statutory authority** with sufficient capacity.

### 2.2.1. THE PERSONAL DATA PROTECTION BILL (PDP BILL), 2019

**Why in News?**

A Joint Parliamentary Committee (JPC) has finalised and adopted the draft report on The Personal Data Protection Bill (PDP Bill), 2019.

**More on News**

- **PDP Bill was first brought in 2019 and was referred to the JPC** for examination at the time.
  - Provisions of the PDP Bill, 2019 are based on the recommendations of the report of the Expert Committee (Chair: Justice B. N. Srikrishna).

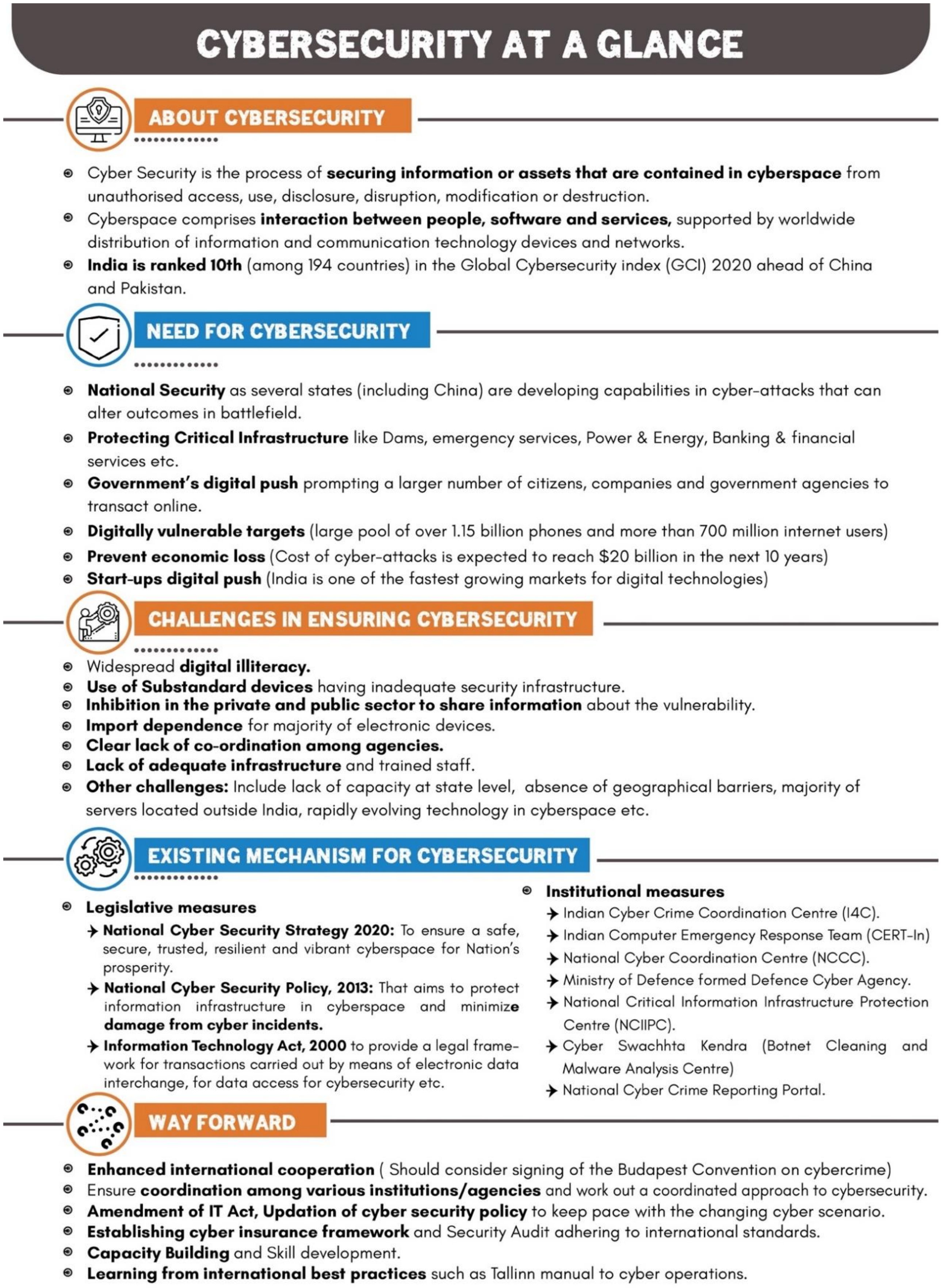
### Personal Data Protection Bill (PDP Bill), 2019

| Provision | Key features of Personal Data Protection Bill (PDP Bill), 2019 | Recommendations by JPC |
|---|---|---|
| **Personal data (data that can identify an individual)** | • It talks about **various types of personal data,** such as<br>○ **Sensitive personal data** (related to finances, health, sex life, caste or tribe, religious or political belief etc.).<br>○ **Critical personal data** (military or national security data and the government can define it from time to time).<br>○ **General personal data-** other than sensitive and critical personal data. | • **Non-personal data should also be included** within the ambit of the law. |
| **Applicability** | • Bill **governs the processing of personal data by**<br>○ Government<br>○ Companies incorporated in India<br>○ Foreign companies dealing with personal data of individuals in India. | |
| **Obligations of data fiduciary (an entity or individual who collects and decides the means and purpose of processing personal data)** | • Personal data **can be processed only for specific, clear and lawful purpose.**<br>• All **data fiduciaries must undertake certain transparency and accountability measures** such as:<br>○ Implementing security safeguards.<br>○ Instituting grievance redressal mechanisms. | • Companies will need to **report a data breach within 72 hours.**<br>• **Mandatorily disclose** if information relating to a data principal is **passed on to someone else.**<br>• **Additional compliance** for companies that deal **exclusively with children's data.** |
| **Rights of the data principal (the individual whose data is being collected and processed)** | • **These include the right to**<br>○ **Obtain confirmation from the fiduciary** on whether their personal data has been processed.<br>○ **Restrict continuing disclosure** of their personal data if it is no longer necessary or consent is withdrawn.<br>○ It also includes the **right to be forgotten which will allow users to erase their personal data** published online. | • **No changes to Section which allows the processing of personal data without a person's consent** if this is necessary, among other things, **for provision of services or benefits from the government,** or issue of licences/certifications/permits from the government for any action or activity. |
| **Social media intermediaries** | • The Bill defines these to include intermediaries **which enable online interaction between users and allow for sharing of information.**<br>○ All such intermediaries which have users above a notified threshold, and whose actions can impact electoral democracy or public order, have certain obligations, which include providing a voluntary user verification mechanism for users in India. | ○ No social media platform should be allowed to operate unless the **parent company handling the technology sets up an office in India.**<br>○ **All social media platforms,** which do not act as intermediaries, **should be treated as publishers** and be held accountable for the content they host.<br>○ **A statutory media regulatory authority,** on the lines of the Press Council of India, may be set up. |
| **Data Protection Authority (DPA)** | • Bill sets up a DPA **which may take steps to protect interests of individuals, prevent misuse of personal data,** and ensure compliance with the Bill. | • DPA **should be bound by directions of the Union government in all cases** – not just questions of policy. |
| **Transfer of data outside India** | ○ **Sensitive personal data may be transferred outside India for processing** if explicitly consented to by the individual and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India.<br>○ **Critical personal data can only be processed in India.** | • Central Government must prepare and **pronounce an extensive policy on data transfer.**<br>• Ensure that **copies of sensitive and critical personal data** already in possession of foreign entities **be brought back in a time-bound manner.** |

| | | |
|---|---|---|
| | ○ Personal data other than sensitive and critical personal data don't have such mandates. | • Development of an alternative **indigenous financial system for cross-border payments** on the lines of Ripple (U.S.) and INSTEX (E.U.).<br>• Government should make efforts to establish a mechanism for the **formal certification process for all digital and IoT devices**. |
| **Exemptions** | ○ **The central government can exempt any of its agencies from the provisions of the Act:**<br>✓ In interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states.<br>✓ For preventing incitement to commission of any offence relating to the above matters.<br>○ **Processing of personal data is also exempted from provisions of the Bill for certain other purposes such as:**<br>✓ prevention, investigation, or prosecution of any offence<br>✓ personal, domestic<br>✓ journalistic purposes | • **Public order should be removed as a ground** for exemption.<br>• There should be **judicial or parliamentary oversight** for granting such exemptions.<br>• There should be an order in writing with reasons for exempting a certain agency from the ambit of the Bill. |

# 3. CYBER SECURITY

## 3.1. CYBER SECURITY



### CYBERSECURITY AT A GLANCE

#### ABOUT CYBERSECURITY

- 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.

#### NEED FOR CYBERSECURITY

- **National Security** as several states (including China) are developing capabilities in cyber-attacks that can alter outcomes in battlefield.
- **Protecting Critical Infrastructure** like Dams, emergency services, Power & Energy, Banking & financial services etc.
- **Government's digital push** prompting a larger number of citizens, companies and government agencies to transact online.
- **Digitally vulnerable targets** (large pool of over 1.15 billion phones and more than 700 million internet users)
- **Prevent economic loss** (Cost of cyber-attacks is expected to reach $20 billion in the next 10 years)
- **Start-ups digital push** (India is one of the fastest growing markets for digital technologies)

#### CHALLENGES IN ENSURING CYBERSECURITY

- Widespread **digital illiteracy.**
- **Use of Substandard devices** having inadequate security infrastructure.
- **Inhibition in the private and public sector to share information** about the vulnerability.
- **Import dependence** for majority of electronic devices.
- **Clear lack of co-ordination among agencies.**
- **Lack of adequate infrastructure** and trained staff.
- **Other challenges:** Include lack of capacity at state level, absence of geographical barriers, majority of servers located outside India, rapidly evolving technology in cyberspace etc.

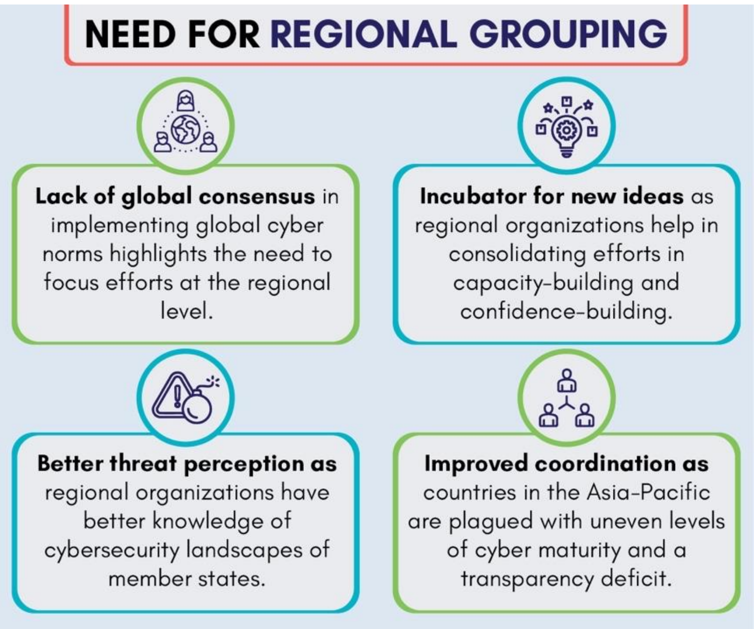
#### EXISTING MECHANISM FOR CYBERSECURITY

- **Legislative measures**
  - **National Cyber Security Strategy 2020:** To ensure a safe, secure, trusted, resilient and vibrant cyberspace for Nation's prosperity.
  - **National Cyber Security Policy, 2013:** That aims to protect information infrastructure in cyberspace and minimize **damage from cyber incidents.**
  - **Information Technology Act, 2000** to provide a legal framework for transactions carried out by means of electronic data interchange, for data access for cybersecurity etc.
- **Institutional measures**
  - Indian Cyber Crime Coordination Centre (I4C).
  - Indian Computer Emergency Response Team (CERT-In)
  - National Cyber Coordination Centre (NCCC).
  - Ministry of Defence formed Defence Cyber Agency.
  - National Critical Information Infrastructure Protection Centre (NCIIPC).
  - Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)
  - National Cyber Crime Reporting Portal.

#### WAY FORWARD

- **Enhanced international cooperation** ( Should consider signing of the Budapest Convention on cybercrime)
- Ensure **coordination among various institutions/agencies** and work out a coordinated approach to cybersecurity.
- **Amendment of IT Act, Updation of cyber security policy** to keep pace with the changing cyber scenario.
- **Establishing cyber insurance framework** and Security Audit adhering to international standards.
- **Capacity Building** and Skill development.
- **Learning from international best practices** such as Tallinn manual to cyber operations.

## 3.1.1. REGIONAL CYBER SECURITY



NEED FOR REGIONAL GROUPING

**Lack of global consensus** in implementing global cyber norms highlights the need to focus efforts at the regional level.

**Incubator for new ideas** as regional organizations help in consolidating efforts in capacity-building and confidence-building.

**Better threat perception as** regional organizations have better knowledge of cybersecurity landscapes of member states.

**Improved coordination as** countries in the Asia-Pacific are plagued with uneven levels of cyber maturity and a transparency deficit.

### Why in News?

First Colombo Security Conclave Virtual Workshop on Developing Regional Cyber Security Capabilities on Defensive operations, Deep/Dark web handling and Digital Forensics was held recently.

### About Colombo Security Conclave (CSC)

- CSC is the **renamed version of National Security Advisor (NSA) Level Trilateral** on Maritime Security (of 2011) with **India, Sri Lanka, Maldives and Mauritius as members** and **Bangladesh and Seychelles as observer states** and Secretariat at Colombo.
- It helps member nations **to build capacity on common security threats** effectively **through its four pillars of cooperation:**
  - Maritime Safety and Security, Terrorism and Radicalization, Trafficking and Organized Crime and Cyber Security and Protection of Critical Infrastructure.

### Major cybersecurity issues faced by South Asia

- **Digital economy:** Region's digital economy is projected to rise at a massive pace. This makes South Asian nations more prone to cyberattacks.
- **Knowledge gap:** i.e. lack of practical guidance on existing good practices, policies, security baselines, and frameworks relating to cybersecurity.
- **Lacking capabilities and infrastructure:** related to cybersecurity in many South Asian countries Region also has a shortage of trained cybersecurity professionals.
- **Lack of regional coordination:** often because of mistrust and a lack of transparency. Absence of a unifying framework often results in significant underinvestment.
- **Rapid technological advancement:** It makes threat monitoring and response more difficult.
- **Potential use by states:** A number of States are developing ICT capabilities for military purposes.
- **Threat from non-state actors:** including criminal groups and terrorists, their differing motives may threaten regional peace and security.

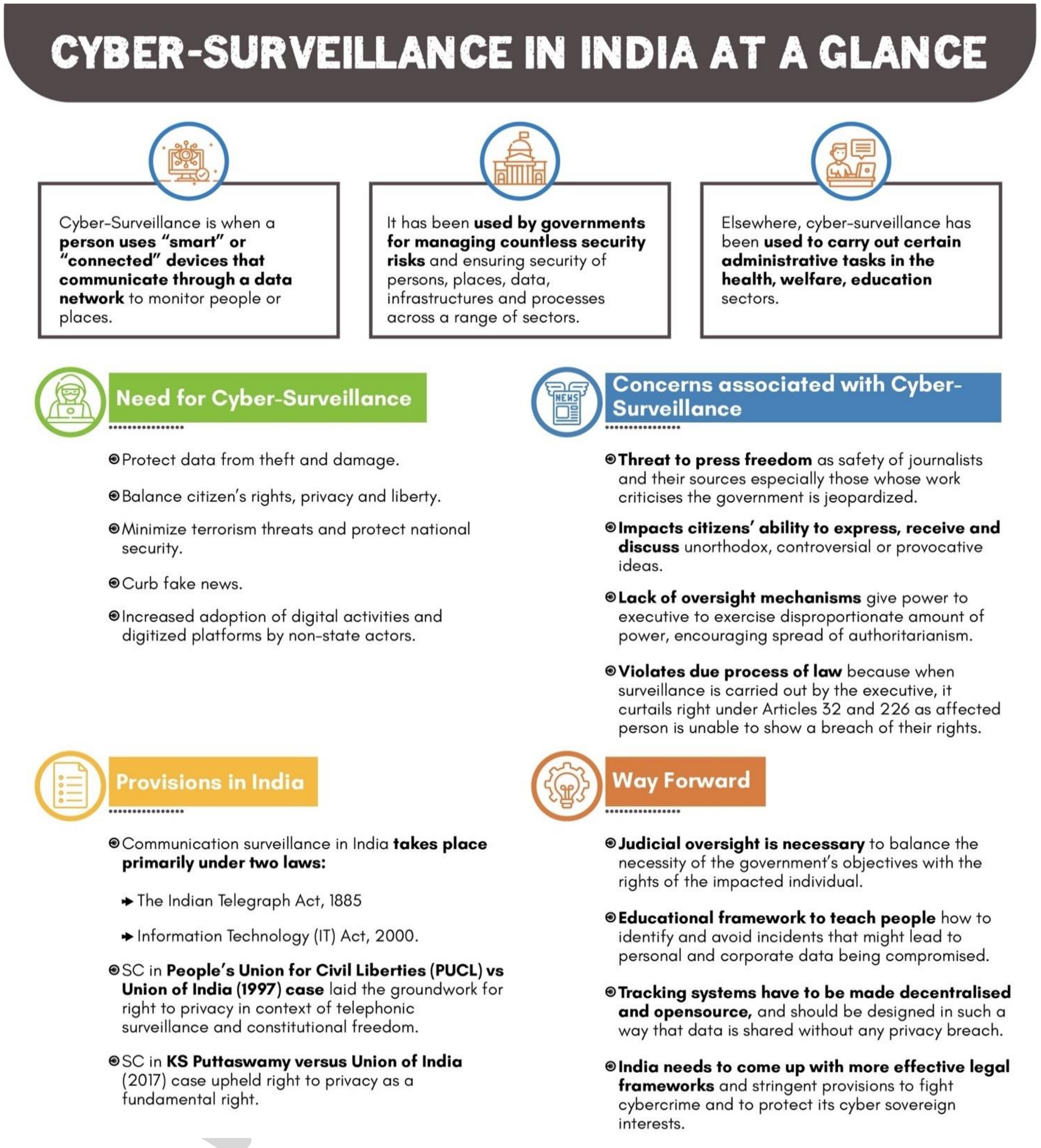
**Some Initiatives taken at regional level**

- **Pacific Cyber Security Operational Network (PaCSON)** for sharing cybersecurity threat information and tools between the member states.
- **ASEAN members** agreed to subscribe in principle to the 11 voluntary, non-binding norms recommended by the 2015 **Report of the U.N. Group of Governmental Experts (UNGGE).**
- **Singapore-ASEAN Cybersecurity Centre of Excellence (ASCCE)** helps to foster a common understanding of cybersecurity through technical capacity-building.
- **YAKSHA, an EU-ASEAN partnership** that develops cybersecurity solutions tailored to specific national needs leveraging EU Know-How and local knowledge.

### Way forward

- **Cyber norm implementation should be prioritized** in regional organizations **through a multi-stakeholder approach.**
- Regional endeavors should **enhance cooperation with relevant capacity-building organizations,** such as the Global Forum on Cyber Expertise (GFCE), to focus protection of critical infrastructure, information sharing etc.
- **Launching awareness-raising campaigns** for educating mainstream users about basic cybersecurity hygiene.
- **Increased responsibility of relevant actors** in adopting dynamic management of cybersecurity (vulnerability management, vulnerability handling etc.).
- **Ensuring harmonization** across emerging national regulatory and industry approaches; creating incentives for security-focused behavior for both the public and private sector.

## 3.2. CYBER SURVEILLANCE IN INDIA



CYBER-SURVEILLANCE IN INDIA AT A GLANCE

Cyber-Surveillance is when a **person uses "smart" or "connected" devices that communicate through a data network** to monitor people or places.

It has been **used by governments for managing countless security risks** and ensuring security of persons, places, data, infrastructures and processes across a range of sectors.

Elsewhere, cyber-surveillance has been **used to carry out certain administrative tasks in the health, welfare, education** sectors.

**Need for Cyber-Surveillance**

- Protect data from theft and damage.
- Balance citizen's rights, privacy and liberty.
- Minimize terrorism threats and protect national security.
- Curb fake news.
- Increased adoption of digital activities and digitized platforms by non-state actors.

**Concerns associated with Cyber-Surveillance**

- **Threat to press freedom** as safety of journalists and their sources especially those whose work criticises the government is jeopardized.
- **Impacts citizens' ability to express, receive and discuss** unorthodox, controversial or provocative ideas.
- **Lack of oversight mechanisms** give power to executive to exercise disproportionate amount of power, encouraging spread of authoritarianism.
- **Violates due process of law** because when surveillance is carried out by the executive, it curtails right under Articles 32 and 226 as affected person is unable to show a breach of their rights.

**Provisions in India**

- Communication surveillance in India **takes place primarily under two laws:**
  - The Indian Telegraph Act, 1885
  - Information Technology (IT) Act, 2000.
- SC in **People's Union for Civil Liberties (PUCL) vs Union of India (1997) case** laid the groundwork for right to privacy in context of telephonic surveillance and constitutional freedom.
- SC in **KS Puttaswamy versus Union of India** (2017) case upheld right to privacy as a fundamental right.

**Way Forward**

- **Judicial oversight is necessary** to balance the necessity of the government's objectives with the rights of the impacted individual.
- **Educational framework to teach people** how to identify and avoid incidents that might lead to personal and corporate data being compromised.
- **Tracking systems have to be made decentralised and opensource,** and should be designed in such a way that data is shared without any privacy breach.
- **India needs to come up with more effective legal frameworks** and stringent provisions to fight cybercrime and to protect its cyber sovereign interests.

## 3.3. THE CRIMINAL PROCEDURE (IDENTIFICATION) ACT, 2022

**Why in news?**

Recently, the **Criminal Procedure (Identification) Act, 2022** received President's assent.

**About the Act**

- The Act seeks to **replace the Identification of Prisoners Act, 1920**.
  - **Law Commission of India (1980) and Malimath Committee (2003)** also recommended need to revise the act to bring it **in line with modern trends** in criminal investigation.
- **Objective:** To expand the **scope and ambit of the "measurements"** which can be taken under the provisions of law that will help in **unique identification of a person** involved in any crime and will **assist the investigating agencies.**

### Key Features of the Act

- **Expands the ambit (Refer table):** Act **expands** the **type of data** that may be collected, **persons from whom such data** may be collected, and the **authority that may authorise** such collection.
- **Retention of details:** Act requires the details collected to be retained in digital or electronic form for 75 years from the date of collection.
- **Powers of Magistrate:** Under the Act, a Magistrate may direct a person to give details for purpose of an investigation or proceeding under CrPC.
- **Rule-making power extended to the central government.**

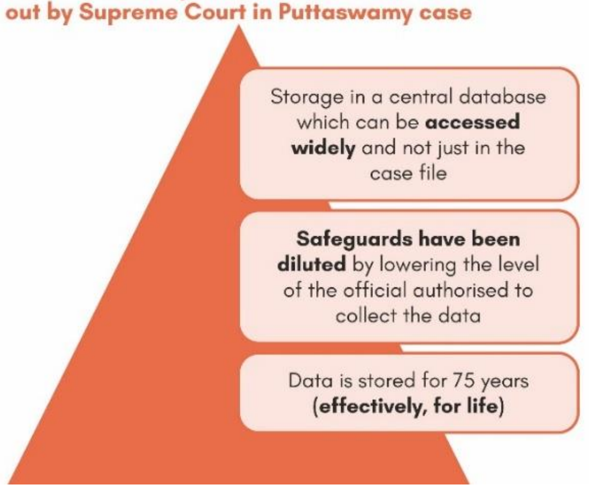
### Comparison of key provisions of the 1920 Act and the 2022 Act

| | 1920 Act | Changes in the 2022 Act |
|---|---|---|
| **Data permitted to be collected** | • Fingerprints, foot-print impressions, photographs. | • Iris and retina scan, physical, biological samples and their analysis, behavioural attributes including signatures, handwriting or any other examination referred to in section 53 or section 53A of CrPC, 1973. |
| **Persons whose data may be collected** | • Convicted or arrested for offences punishable with **rigorous imprisonment of one year or more.**<br>• Persons **ordered to give security** for good behaviour or maintaining peace.<br>• Magistrate **may order in other cases** collection **from any arrested person** to aid criminal investigation. | • **Convicted or arrested** for any offence. However, biological samples may be taken **forcibly** only from persons arrested for offences **against a woman or a child**, or if the offence carries a **minimum of seven years imprisonment.**<br>• **Persons detained** under any preventive detention law.<br>• On the order of Magistrate, **from any person** (not just an arrested person) **to aid investigation.** |
| **Persons who may require/ direct collection of data** | • Investigating officer, officer in charge of a police station, or of rank Sub-Inspector or above.<br>• Magistrate. | • **Officer in charge** of a police station, or of **rank Head Constable** or above. In addition, a Head Warden of a prison.<br>• **Metropolitan Magistrate** or **Judicial Magistrate** of first class. In case of persons required to maintain good behaviour or peace, the **Executive Magistrate.** |

### Concerns about the Act

- **Violate right to privacy** (Refer infographic).
- **Differs from Law commission observation:** Act expands the set of persons whose data may be collected and also **expands the power of the Magistrate** to order collection from any person.
- **Other issues:**
  - **No standardised norms for collection** are prescribed for individuals who will be collecting the measurements.
  - **NCRB is ill-equipped** to deal with quality management for a database containing records of the proposed measurements, particularly of **biological samples and their analysis.**
  - **No limitations on the use** of the data collected and the term **"analysis" is left undefined.**

Provisions that may not meet the standards laid out by Supreme Court in Puttaswamy case



Storage in a central database which can be **accessed widely** and not just in the case file

**Safeguards have been diluted** by lowering the level of the official authorised to collect the data

Data is stored for 75 years **(effectively, for life)**

### Conclusion

A law **that restricts fundamental rights** must be sufficiently **clear and precise** in terms of the **extent, scope and nature** of the interference allowed, along with the **presence of sufficient safeguards** to prevent abuse of powers by authorities.

## 3.3.1. FACIAL RECOGNITION TECHNOLOGY (FRT)

### Why in News?

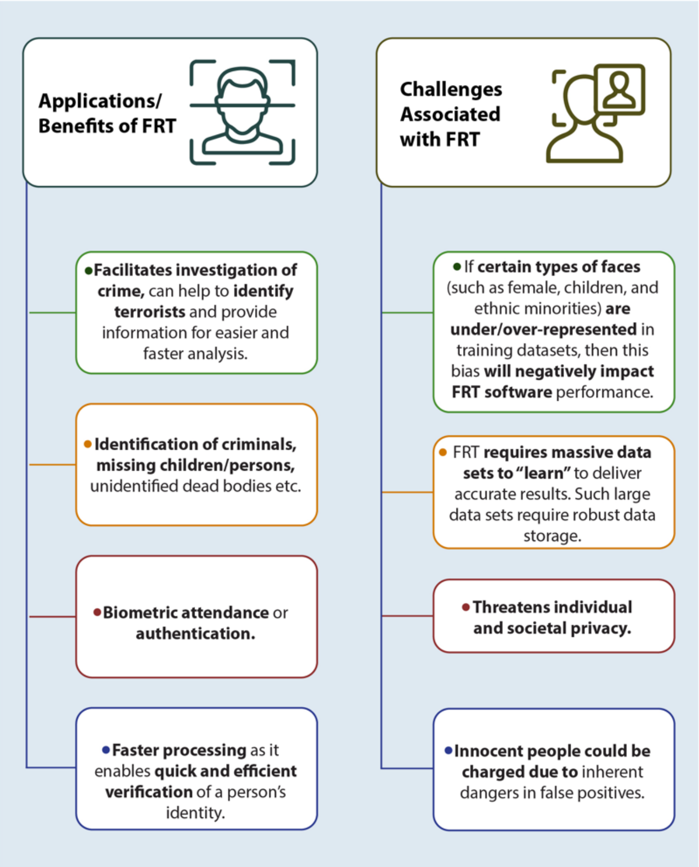
Recently, government stated that Facial Recognition Technology (FRT) will be introduced at 4 airports soon.

### About FRT

- Facial recognition is the process of **identifying or verifying the identity of a person using their face.**
- It relies on many of the processes and techniques **associated with AI.**
- It captures, analyzes, and compares patterns based on the person's facial details. It may involve **Face detection, Face capture and Face match**.
- It also has the **ability to gather demographic data on crowds.**

### Way forward

- **Need of a clear law**: In the interest of civil liberties and to save democracy from turning authoritarian.
- **Required Expertise in the field**: Experts are needed to verify 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.



**Applications/ Benefits of FRT**

- **Facilitates investigation of crime,** can help to **identify terrorists** and provide information for easier and faster analysis.
- **Identification of criminals, missing children/persons,** unidentified dead bodies etc.
- **Biometric attendance** or **authentication.**
- **Faster processing** as it enables **quick and efficient verification** of a person's identity.

**Challenges Associated with FRT**

- If **certain types of faces** (such as female, children, and ethnic minorities) **are under/over-represented** in training datasets, then this bias **will negatively impact FRT software** performance.
- FRT **requires massive data sets to "learn"** to deliver accurate results. Such large data sets require robust data storage.
- **Threatens individual and societal privacy.**
- **Innocent people could be charged due to** inherent dangers in false positives.

**International practices**

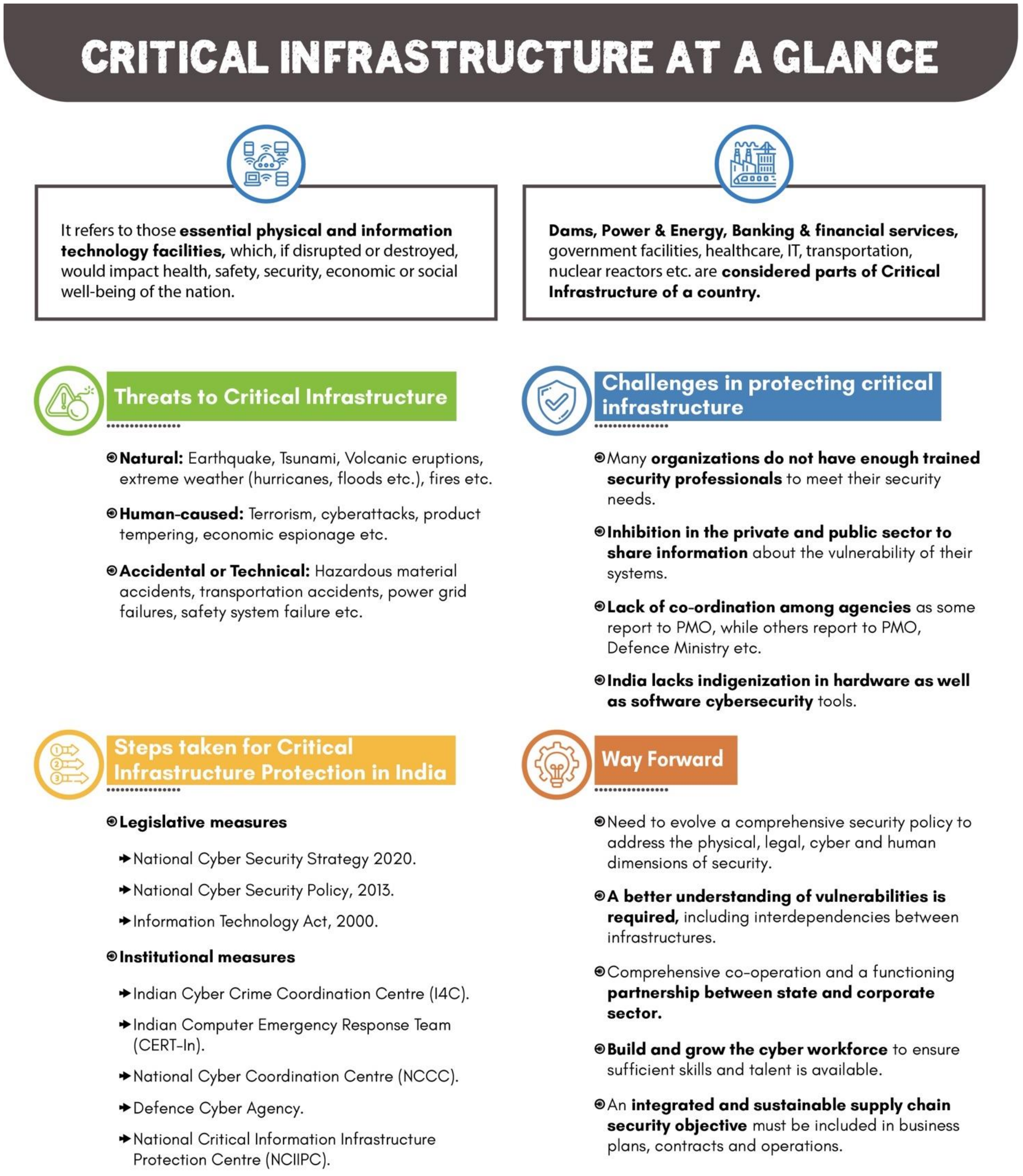
- **United States**: FBI uses facial recognition technology for potential investigative leads.
- **United Kingdom**: police forces in England use facial recognition to tackle serious violence.
- **China:** It uses facial recognition for racial profiling and mass surveillance in order to track Uighur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

**Related information**

**Government has approved implementation of National Automated Facial Recognition System (NAFRS).**

- NAFRS is to be **used by police pan-India** and will be issued by 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.

## 3.4. CRITICAL INFRASTRUCTURE



### CRITICAL INFRASTRUCTURE AT A GLANCE

It refers to those **essential physical and information technology facilities,** which, if disrupted or destroyed, would impact health, safety, security, economic or social well-being of the nation.

**Dams, Power & Energy, Banking & financial services,** government facilities, healthcare, IT, transportation, nuclear reactors etc. are **considered parts of Critical Infrastructure of a country.**

#### Threats to Critical Infrastructure

- **Natural:** Earthquake, Tsunami, Volcanic eruptions, extreme weather (hurricanes, floods etc.), fires etc.
- **Human-caused:** Terrorism, cyberattacks, product tempering, economic espionage etc.
- **Accidental or Technical:** Hazardous material accidents, transportation accidents, power grid failures, safety system failure etc.

#### Challenges in protecting critical infrastructure

- Many **organizations do not have enough trained security professionals** to meet their security needs.
- **Inhibition in the private and public sector to share information** about the vulnerability of their systems.
- **Lack of co-ordination among agencies** as some report to PMO, while others report to PMO, Defence Ministry etc.
- **India lacks indigenization in hardware as well as software cybersecurity** tools.

#### Steps taken for Critical Infrastructure Protection in India

- **Legislative measures**
  - National Cyber Security Strategy 2020.
  - National Cyber Security Policy, 2013.
  - Information Technology Act, 2000.
- **Institutional measures**
  - Indian Cyber Crime Coordination Centre (I4C).
  - Indian Computer Emergency Response Team (CERT-In).
  - National Cyber Coordination Centre (NCCC).
  - Defence Cyber Agency.
  - National Critical Information Infrastructure Protection Centre (NCIIPC).

#### 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.
- Comprehensive co-operation and a functioning **partnership between state and corporate sector.**
- **Build and grow the cyber workforce** to ensure sufficient skills and talent is available.
- An **integrated and sustainable supply chain security objective** must be included in business plans, contracts and operations.

### 3.4.1. CYBER SECURITY IN POWER SECTOR

**Why in News?**

Recently, Government has released guidelines for the **Cyber Security in Power Sector**.

**More about news**

- **Central Electricity Authority** has framed **Guideline on Cyber Security in Power Sector** to be adhered by all Power Sector utilities to **create cyber secure eco system.**

- This is the first time that a comprehensive guideline has been formulated on cyber security in power sector.
- The **guideline lays down actions required to ramp up security measures** across various utilities to raise preparedness in power sector.
- These **Guideline are mandatory requirements** to be met by all stakeholders and lay emphasis on:
  - **Establishing cyber hygiene,**
  - **Training of all IT as well OT Personnel on Cyber Security,**
  - **Designating of Cyber Security Training Institutes**
  - **Cyber Testing labs** in the Country
- The Guideline **mandates ICT based procurement 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 when system for trusted product and service is in place.

**Related Information**

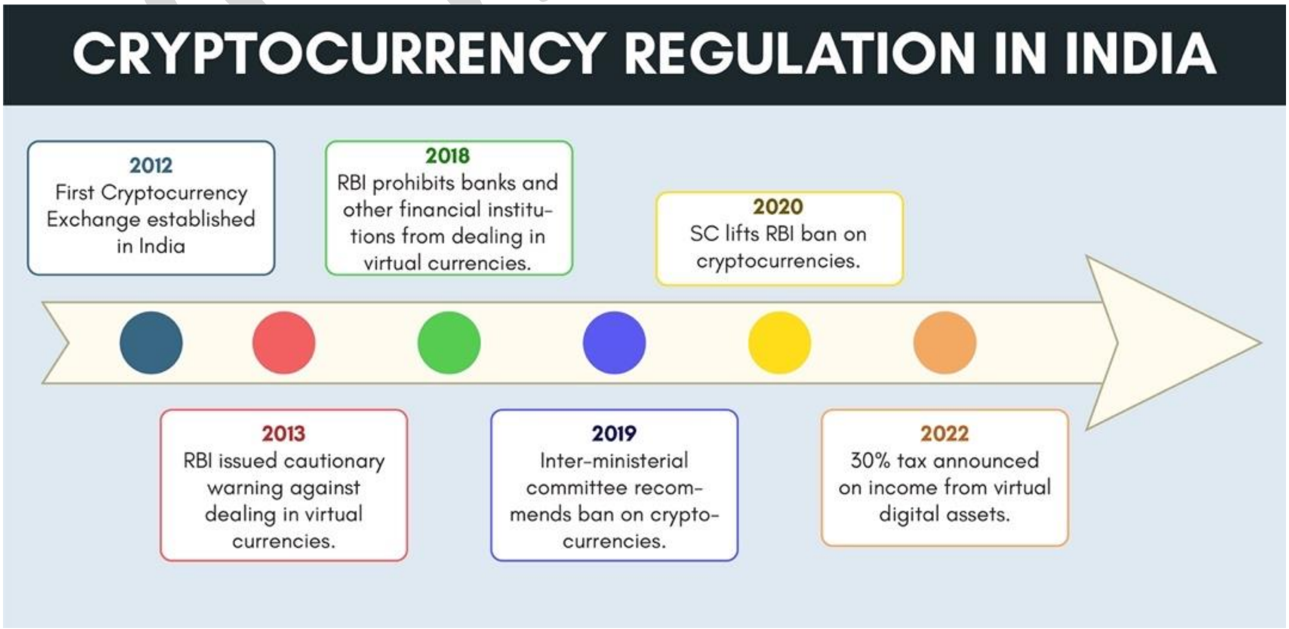
**National Security Directive on the Telecom Sector (NSDTS)**

- Indian directives for telecom security **come** (in December 2020) **amid global security concerns raised against Chinese equipment maker Huawei.**
  - Need was felt because of concerns like **cyber security, national security, dubious telecom equipment suppliers, realizing self-reliance** etc.
- 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 NSDTS, **government declares a list of trusted sources and trusted products** for installation in the country's telecom network.
  - List will be decided **based on approval of National Security Committee on Telecom** headed by deputy national security advisor
- 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.
- New devices have to be **mandatorily procured from trusted sources.**
- Later in June 2021, government **under NSDTS launched Trusted Telecom Portal (TTP) for giving clearance to trusted products** that telecom service providers (TSPs) can install in their network.

## 3.5. CRYPTOCURRENCY CRIMES

**Why in news?**

Recently, for the first time **Bureau of Police Research and Development (BPRD)** has **issued a standard operating procedure for law enforcement agencies** in India on how to probe crypto crimes, and seize and preserve cryptocurrencies during investigation.



CRYPTOCURRENCY REGULATION IN INDIA

2012 First Cryptocurrency Exchange established in India

2013 RBI issued cautionary warning against dealing in virtual currencies.

2018 RBI prohibits banks and other financial institutions from dealing in virtual currencies.

2019 Inter-ministerial committee recommends ban on cryptocurrencies.

2020 SC lifts RBI ban on cryptocurrencies.

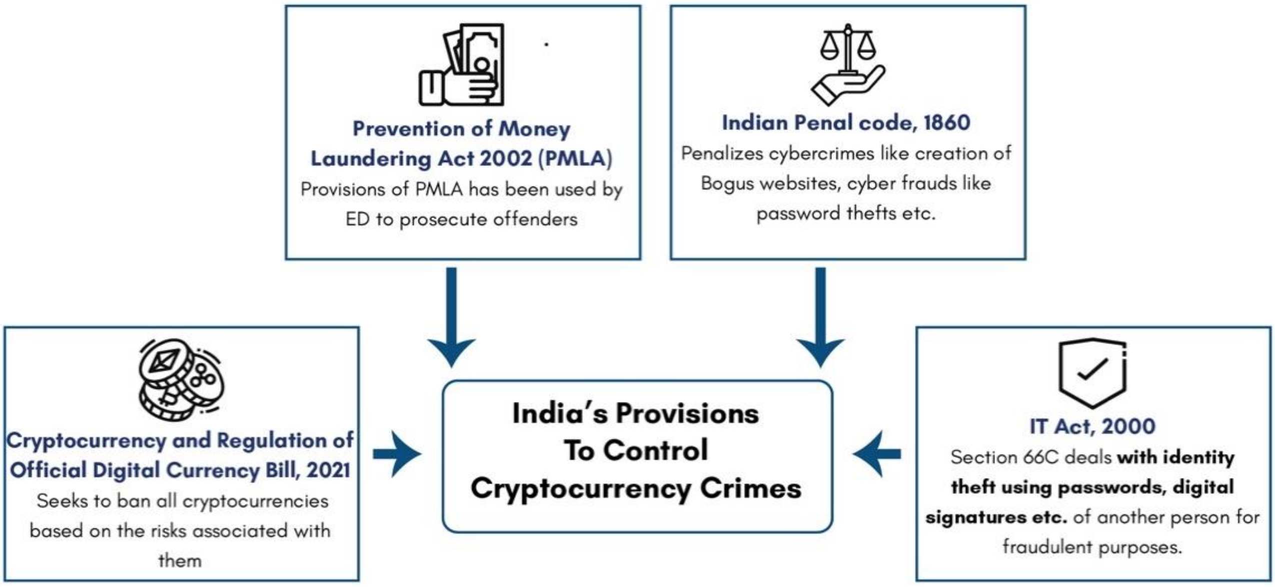
2022 30% tax announced on income from virtual digital assets.

### More about news

- In 2021, **illicit transactions** using cryptocurrencies were **estimated to be $14 billion**, 79% increase from $7.8 billion the previous year.
- Currently, there are **no national guidelines on cryptocurrency related cases**, due to which enforcement agencies often struggle, particularly in seizure as well as tracing suspects.
- Cryptocurrency and the exchanges where digital currency can be traded anonymously have emerged as **key tools for the cyber extortionists.**

### How cryptocurrency is threat to the nation?

- **Internal security**:
  - **Terrorism:** There is wider use of cryptocurrencies on the dark net for terror acts and drug trafficking by militant organisations.
  - **Money Laundering**: Cryptocurrency market isn't universally protected or regulated like Banks, thus is **increasingly used to launder money**.
  - Cryptocurrency is sometimes **used as payment for extortion** because the money trail is difficult to trace.
  - Anonymity offered by the cryptocurrency ecosystem **makes it difficult for tax authorities to trace transactions** to individuals and verify their tax liabilities.
- **Individual:** Criminals can infect individual computers with malware that steals cryptocurrency as well as steal personal information and data.
- **Environment:** Crypto miners employ sophisticated, energy intensive machines and energy used has a large portion come from coal-fired power plants.
- **Investment risk:** as Cryptocurrencies have no fundamental value, and therefore could drop to zero at any time.



**Prevention of Money Laundering Act 2002 (PMLA)**
Provisions of PMLA has been used by ED to prosecute offenders

**Indian Penal code, 1860**
Penalizes cybercrimes like creation of Bogus websites, cyber frauds like password thefts etc.

**Cryptocurrency and Regulation of Official Digital Currency Bill, 2021**
Seeks to ban all cryptocurrencies based on the risks associated with them

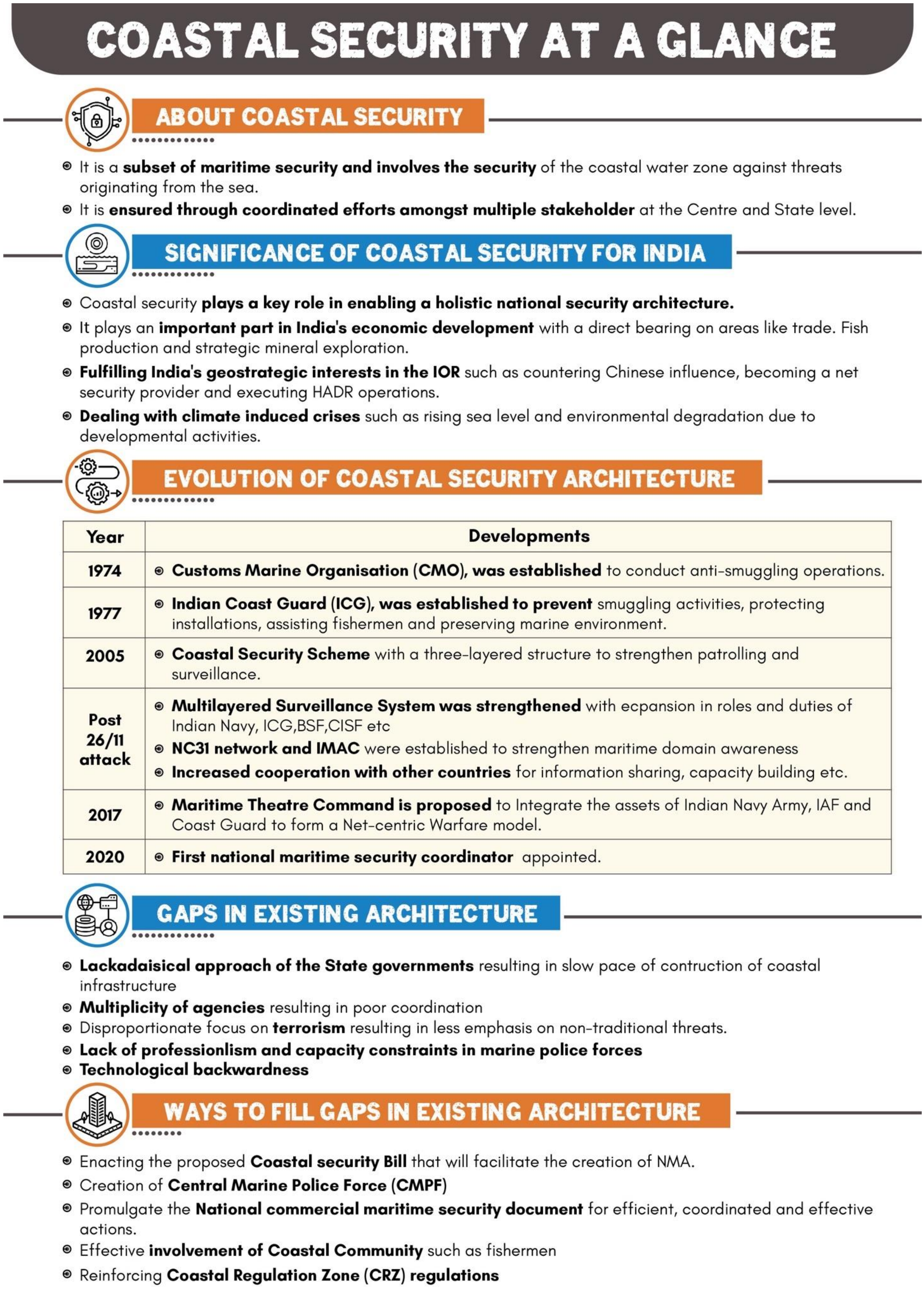
**India's Provisions To Control Cryptocurrency Crimes**

**IT Act, 2000**
Section 66C deals **with identity theft using passwords, digital signatures etc.** of another person for fraudulent purposes.

### Way forward

- **Individual Crypto wallet**: As per BPRD guidelines, law enforcement agencies must have their own crypto wallet to store seized virtual digital assets, and they need for liaise with crypto exchanges to block a suspect's wallet or resetting the keys to defuse transactions in an ongoing investigation.
- **Proper regulations**: Regulatory and financial bodies should develop regulations to minimize risk and increase compliance in a constantly and fast-growing crypto asset industry.
- **Fraud detection**: Blockchain technologies should implement automated Anti Money Laundering (AML) fraud detection that would block or flag suspicious transactions prior to them being carried out.
- **Legal framework:** There is urgent need to have a Cryptocurrency Regulation Bill in India to regulate and deal with cryptocurrency crimes.
- **Awareness**: There is need to educate and inform people to reduce the risk associated with cryptocurrency theft.

# 4. COASTAL SECURITY



## 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** with a three-layered structure to strengthen patrolling and surveillance. |
| Post 26/11 attack | **Multilayered Surveillance System was strengthened** with ecpansion in roles and duties of Indian Navy, ICG,BSF,CISF etc<br>**NC31 network and IMAC** were established to strengthen maritime domain awareness<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. |
| 2020 | **First national maritime security coordinator** appointed. |

### 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**

### WAYS TO FILL GAPS IN EXISTING ARCHITECTURE

- Enacting the proposed **Coastal security Bill** that will facilitate the creation of NMA.
- 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**

# 5. POLICING REFORMS

## 5.1. MODERNISATION OF POLICE FORCE

### MODERNISATION OF POLICE FORCE AT A GLANCE

In India, police and law and order **come under the purview of state governments.**

However, due to **financial constraints States have not been able to fully modernize** their police forces.

Therefore, **MHA has been supplementing efforts and resources of the States** through Modernisation of State Police Forces Scheme.

### NEED FOR POLICE MODERNISATION

- **New types of crime,** based on technology, are being invented (ransomware, dark web etc.).
- To **include modern technology into investigation** and enforcement.
- **Combating transnational organized crimes** that are often complex and multijurisdictional.

### STEPS TAKEN

- **Modernisation of Police Forces scheme provides for**
  - Provision of **internal security, law and order, adoption of modern technology** by Police.
  - Independent **high-quality forensic sciences facilities** in States/UTs.
  - **Security related expenditure for Jammu & Kashmir,** insurgency affected North Eastern States and Left Wing Extremism (LWE) affected area.
- **SMART policing**
- **Crime and Criminal Tracking Network System (CCTNS)**
- **Model Police Act, 2006**

### ISSUES FACED IN MODERNISATION

- Even at present, police are based on colonial laws like **Indian Police Act, 1861.**
- **Politicization of police.**
- **Overburdened police force.**
- **Infrastructural issues:** Lack of resources (Weaponry, connectivity, etc.), Lack of technology use etc.

### WAY FORWARD

- State police forces **should be provided with modern sophisticated weaponry** and proper training to handle those.
- **Use of advanced technologies** like biometric identification, facial recognition, CCTV cameras, GPS, forensic science, etc.
- **Need to upgrade the existing cyber cells** by setting up dark web monitoring cells and social media monitoring cells.
- **Annual actions plans** to address deficit in infrastructural requirements.
- Remove bottlenecks and **conduct Police recruitment drives** in a mission mode.
- **Implement Seven directives of Supreme Court** in Prakash Singh vs Union of India, 2006.

## 5.2. ROLE OF TECHNOLOGY IN LAW ENFORCEMENT

**Why in news?**

Prime Minister recently called for adoption of future technologies for grass root policing requirements and development of inter-operable technologies which would benefit Police forces across the country.

### TECHNOLOGIES USED IN LAW ENFORCEMENT

**Some common technologies being used for Crime surveillance and** Monitoring include CCTV cameras, Drones and Global Positioning System (GPS). Various other newly emerging technologies are:

**Body-Worn Cameras and In-Car Videos**

- for better evidence documentation, increased accountability and transparency.

**Automatic Tag and License Plate Readers**

- Mounted to the exterior of patrol cars, and instantly analyzes license plates on every vehicle that comes within their range of view.

**Biometrics and Hand- Held Fingerprint Scanners**

- Use of biometrics using unique biological traits such as finger- prints, retina scans, and DNA to identify individuals.

**Brain Fingerprinting**

- Uses brain scans to capture how a crime suspect's brain reacts when being questioned by police.

**Google Glass**

- Mobile interceptors that take photographs of traffic violations and instantly upload them to their police department's system.
- It is **currently being used on the National Highways in India**

**Predictive-Analytics Software**

- It helps find crime patterns and deploy police accordingly.
- Delhi government has recently collaborated with ISRO to start with new technology called **Crime Mapping Analytics and Predictive System (CMAPS).**

**BEST PRACTICES IN INDIA**

**Uttar Pradesh Police**

An **AI enabled app** developed by startup Staqu digitizes and searches records of criminals and their associates and assists police forces with real-time information retrieval during investigations.

**Odisha Police**

An app named, **'MO SAATHI'** helps women who are stuck in dangerous situations to alert the police, make audio and video recording, and send it to the Modern Police Control Room.

**Maharashtra Police**

**An Automated Multimodal Biometric Identification System (AMBIS)** — a digital database of finger prints and photographs of criminals eliminates limitations of manual search on the biometric database.

### Significance of leveraging technology in policing

In India, police to population ratio is less than 150 per 100,000, against the UN recommended 222. Technology therefore can **act as a force multiplier** thereby increasing the efficiency and effectiveness of police in various ways:

- **Improving Public Police interface:** By providing digital access to the police, citizens can avail services from the comfort of their home (Ex: **Saanjh a citizen-facing portal** of Punjab Police).
- **Crime prevention and detection**: Mobile forensics Big Data, AI etc. can be used to identify crime patterns and hot spots, to draw correlations between the type of crime, time, location etc.
    - Recently, Government has approved implementation of the **National Automated Facial Recognition System (NAFRS)** to facilitate crime investigation and identifying a criminal regardless of face mask, makeup etc.
- **Awareness generation:** Social media can be used by law enforcement agencies to reach out directly to citizens —how to protect against cybercrime, dispelling rumors, countering fake news etc.

**Challenges in extensive use of technologies**

**Breach of privacy**

Excessive use of tecnology in criminal investigations has also led to a situation where police get into personal information, not relevant to the investigation.

**Absence of regulation**

In the absence of laws to regulate and specify the procedure for the use of technology, it is left to the police itself as to how this can be used.

**Expensive Affair**

Technology is being updated every day and changing them every now and then would lead to huge expenditure.

**Increased stress for police officials**

There is an inherent amount of stress involved with learning and applying many of the advanced technologies.

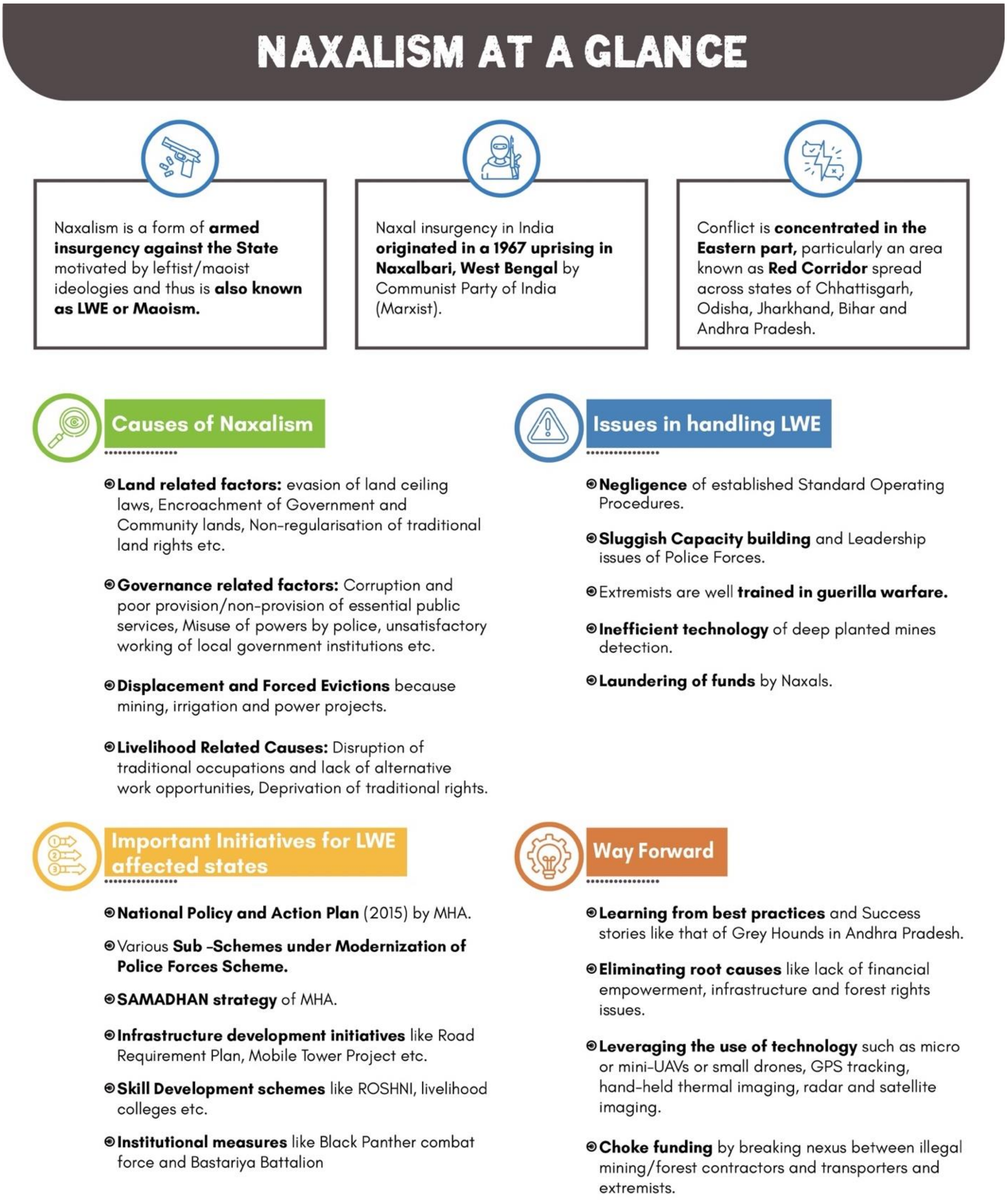
- **Improving Internal Efficiency:** such as the time taken to file a charge-sheet, types of crimes solved, citizen feedback scores can be used to determine an officer's performance in a more objective manner.
- **Real-time integration:** between five pillars of the criminal justice system (police, courts, prosecution, jails and forensics) can significantly increase the efficiency of law enforcement agencies (LEAs).

**Way ahead**

- **Technology adoption needs to be corroborated** by issues being faced by the LEAs such as lack of accountability, poor representation of women and shortage of weaponry.
- **Regulating technologies:** The enactment of the Personal Data Protection Bill 2019 and DNA Technology (Use and Application) Regulation Bill, 2018 must be expedited to bring in regulations for safe use of technology and addressing privacy concerns.
- **Capacity building:** Providing proper time for training officers on new technologies to bring in confidence and reducing stress.
- **Building Digital Trust:** There is a need to imbibe Digital ethics, which is a broader framework that includes technology, transparent data and digital ethics to create digital trust in society.

# 6. EXTREMISM AND TERRORISM

## 6.1. NAXALISM



### NAXALISM AT A GLANCE

Naxalism is a form of **armed insurgency against the State** motivated by leftist/maoist ideologies and thus is **also known as LWE or Maoism.**

Naxal insurgency in India **originated in a 1967 uprising in Naxalbari, West Bengal** by Communist Party of India (Marxist).

Conflict is **concentrated in the Eastern part,** particularly an area known as **Red Corridor** spread across states of Chhattisgarh, Odisha, Jharkhand, Bihar and Andhra Pradesh.

### Causes of Naxalism

- **Land related factors:** evasion of land ceiling laws, Encroachment of Government and Community lands, Non-regularisation of traditional land rights etc.
- **Governance related factors:** Corruption and poor provision/non-provision of essential public services, Misuse of powers by police, unsatisfactory working of local government institutions etc.
- **Displacement and Forced Evictions** because mining, irrigation and power projects.
- **Livelihood Related Causes:** Disruption of traditional occupations and lack of alternative work opportunities, Deprivation of traditional rights.

### Issues in handling LWE

- **Negligence** of established Standard Operating Procedures.
- **Sluggish Capacity building** and Leadership issues of Police Forces.
- Extremists are well **trained in guerilla warfare.**
- **Inefficient technology** of deep planted mines detection.
- **Laundering of funds** by Naxals.

### Important Initiatives for LWE affected states

- **National Policy and Action Plan** (2015) by MHA.
- Various **Sub -Schemes under Modernization of Police Forces Scheme.**
- **SAMADHAN strategy** of MHA.
- **Infrastructure development initiatives** like Road Requirement Plan, Mobile Tower Project etc.
- **Skill Development schemes** like ROSHNI, livelihood colleges etc.
- **Institutional measures** like Black Panther combat force and Bastariya Battalion

### Way Forward

- **Learning from best practices** and Success stories like that of Grey Hounds in Andhra Pradesh.
- **Eliminating root causes** like lack of financial empowerment, infrastructure and forest rights issues.
- **Leveraging the use of technology** such as micro or mini-UAVs or small drones, GPS tracking, hand-held thermal imaging, radar and satellite imaging.
- **Choke funding** by breaking nexus between illegal mining/forest contractors and transporters and extremists.

## 6.2. UAPA (UNLAWFUL ACTIVITIES [PREVENTION] ACT)

### Why in News?

Minister of State for Home Affairs provided data related to banned organizations under UAPA (Unlawful Activities [Prevention] Act, 1967) in the country.

**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 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.

### About UAPA

It 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.

### Provisions of the act

- Act defines "Unlawful activity" and **provides certain powers to government:**
  - Under the Act, Central government can **declare a person or an organization as a terrorist/ terrorist organization.**
  - **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.

**Related News**

Recently **SC ruled that Magistrates can't extend probe under UAPA.**

- Court highlighted that **only a special court designated under UAPA (Section 43-D of UAPA) will be authorised** to deal with the issue of extending the time for filing of charge sheets and that magistrates cannot deal with such cases of extension.
  - SC had given a similar verdict in the **in Bikramjit Singh vs. State of Punjab, 2020.**
  - Special courts are **set up under National Investigation Agency (NIA) Act** and in the absence of such special courts, **with sessions courts.**

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

- **To uproot terrorism, which still poses a significant threat, from India.**
- **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 NIA.

**Challenges of UAPA Act, 2019**

> **Related Information**
>
> **About National Investigation Agency (Amendment) Act 2019**
>
> **Key Amendments**
>
> - **Enhances the scope of Offences:** which are mentioned in the schedule to the Act, such as the Atomic Energy Act, 1962, and the Unlawful Activities Prevention Act, 1967.
>     - This amendment enhances this scope to include other offences like human trafficking; offences related to counterfeit currency or bank notes etc.
> - **Enhances the jurisdiction of the NIA:** as the officers of the NIA will have the power to investigate scheduled offences committed outside India.
> - **Special Courts:** The Act allows the central government to constitute Special Courts for the trial of scheduled offences

- **Vague and unclear definitions**: Act does not define terrorism and definition of 'unlawful activity' and is such that it covers almost every kind of violent act be it political or non-political.
- **Excessive discretionary powers to government**: and no objective criterion has been laid for categorization of an individual 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.
- **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 **3.1% of cases** registered under the UAPA between 2018 and 2020 resulted in conviction.
- **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 a **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.

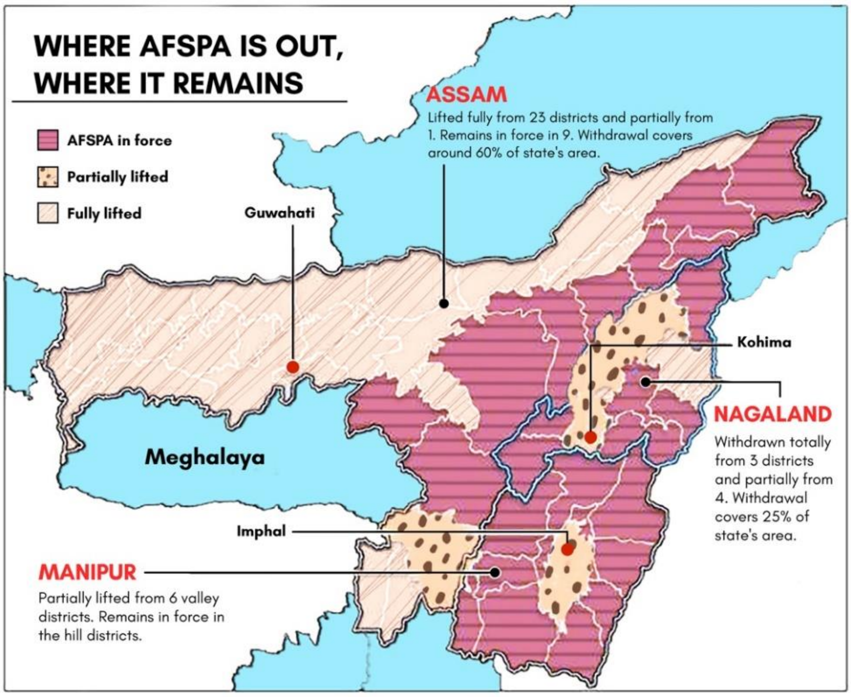
## 6.3. ARMED FORCES SPECIAL POWERS ACT (AFSPA) IN NORTH EAST

**Why in news?**

Recently, the Union Government has partially withdrawn the Armed Forces Special Powers Act (AFSPA), 1958 from parts of three Northeast states— Assam, Nagaland and Manipur.

**About AFSPA**

- AFSPA **grants extra-ordinary powers and immunity to the armed forces** to bring back order in the "disturbed areas".
    - **Central Government or the Governor of the State or administrator of UT can declare** the whole or part of the State or Union Territory as a disturbed area.


WHERE AFSPA IS OUT, WHERE IT REMAINS
AFSPA in force
Partially lifted
Fully lifted
Guwahati
ASSAM
Lifted fully from 23 districts and partially from 1. Remains in force in 9. Withdrawal covers around 60% of state's area.
Kohima
NAGALAND
Withdrawn totally from 3 districts and partially from 4. Withdrawal covers 25% of state's area.
Meghalaya
Imphal
MANIPUR
Partially lifted from 6 valley districts. Remains in force in the hill districts.

- **Section 4 of the AFSPA** empowers armed forces with provisions like **legal immunity for their actions.**
- Presently, AFSPA is operational in **Assam, Jammu and Kashmir and Ladakh, Nagaland, Manipur** (except Imphal Municipal area) and **parts of Arunachal Pradesh.**

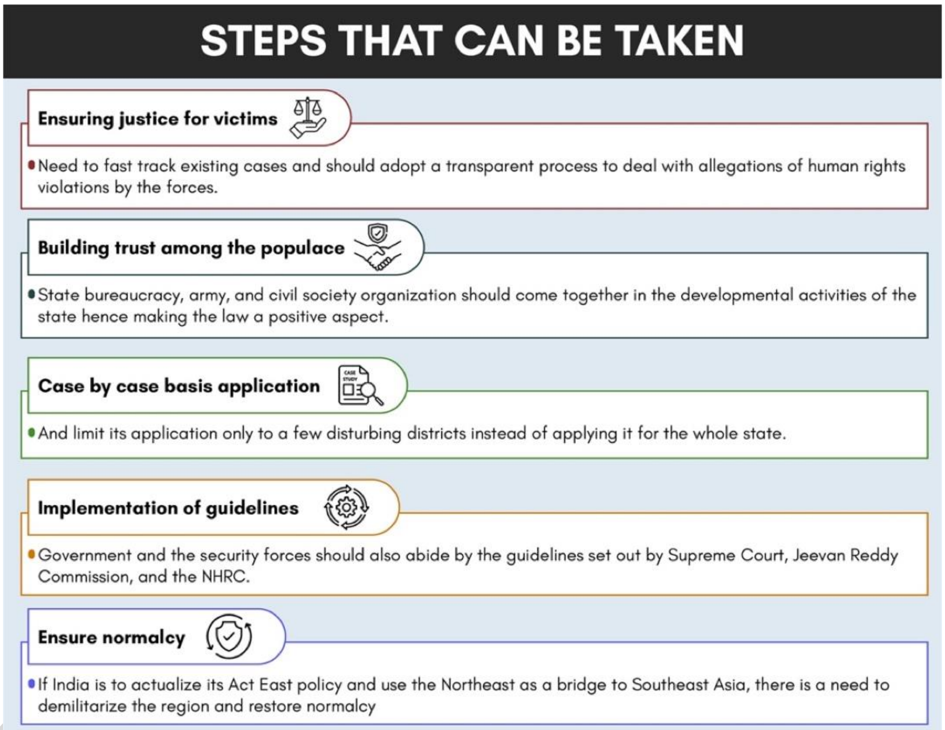
- AFSPA was completely withdrawn in Mizoram in the 1980s, Tripura in 2015 and Meghalaya in 2018

**Significance of the AFSPA**

- **Tool to deal with extraordinary law and order situation:** perpetrated by insurgents spreading terror.
- **Necessary to deal with insurgency:** this makes the deployment of armed forces in a counter-insurgency role with enhanced legal protection necessary.
- **To prevent security gap:** The army needs special powers to tackle homegrown and as well as foreign terrorists. Withdrawal of Army from such areas will create a huge gap in the security grid in sensitive areas.

**Reasons for opposition against AFSPA**

- **Violation of human rights:** there have been multiple allegations of "fake encounters" and other human rights violations by the security forces in 'disturbed' areas.
  - Recently, 14 villagers were killed during an anti-insurgency operation in Nagaland's Mon district.
- **Violation of fundamental rights:** The power of arbitrary arrest and detention given to the armed forces goes against the fundamental right vested in Article 22.
- **Blanket immunity to security personnel.**



STEPS THAT CAN BE TAKEN

**Ensuring justice for victims**

- Need to fast track existing cases and should adopt a transparent process to deal with allegations of human rights violations by the forces.

**Building trust among the populace**

- State bureaucracy, army, and civil society organization should come together in the developmental activities of the state hence making the law a positive aspect.

**Case by case basis application**

- And limit its application only to a few disturbing districts instead of applying it for the whole state.

**Implementation of guidelines**

- Government and the security forces should also abide by the guidelines set out by Supreme Court, Jeevan Reddy Commission, and the NHRC.

**Ensure normalcy**

- If India is to actualize its Act East policy and use the Northeast as a bridge to Southeast Asia, there is a need to demilitarize the region and restore normalcy

**Steps taken by various agencies to reach a middle ground**

| | |
|---|---|
| **Supreme Court Verdicts** | • **Naga People's Movement of Human Rights vs. Union of India(1998):** The Court held that the act cannot be considered as violative of the Constitution.<br>○ However, **the court held that the army personnel are required to strictly follow minimum force.** Also, the act has to be reviewed every six months by the state.<br>• **July 2016 judgement:** SC directed the armed forces and police not to use "excessive or retaliatory force" in even in areas declared 'disturbed' where the AFSPA is applicable.<br>• **July 2017 judgement:** on alleged unlawful encounter killings in Manipur marked an important institutional step when it ordered CBI to set up a special investigation team to probe encounter deaths. |
| **Formation of various committees** | • **B P Jeevan Reddy Committee (2005):** security forces must be brought under the purview of ordinary criminal law rather than under army law.<br>• **Santosh Hegde committee (2013):** need for restraint and stricter mechanism to prevent its misuse or abuse. |
| **Other prominent steps:** | • The **5th report of the Second Administrative Reforms Commission** on public order has also recommended the repeal of the AFSPA.<br>• Both the **National Human Rights Commission and the Supreme Court in 2014 have laid down the guidelines** to be followed by the state in case of encounter deaths.<br>• **Activists such as Irom Sharmila** have protested the existence of the AFSPA. |

**Conclusion**

AFSPA is objected on the grounds that it gives the security forces unbridled powers. However, Army sees it as an enabling Act that gives it the powers necessary to conduct counter-insurgency operations efficiently.

There is a need to find a middle ground, based on SC judgements and various committee's recommendations, where both, the rights of civilians and operational needs of armed forces, are considered.

## 6.4. 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?

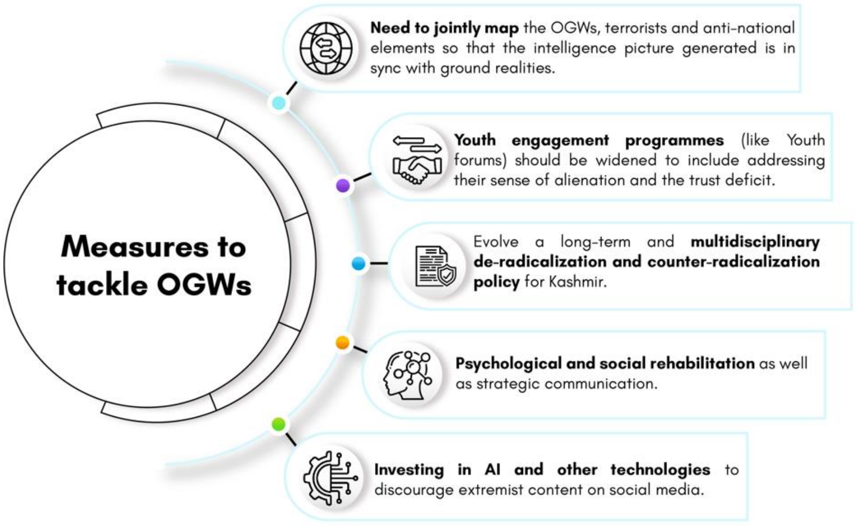
- OGWs are often described as **'militants without weapons" and** have the potential to become future militants. J&K Police categorize **"anybody who supports the militants" as an OGW.**
- They are generally recruited by employing a strategy of **systematic entrapment** which starts out with radicalization of youth, which progresses into more serious crimes and culminates into being an OGW.
  - Terror groups like Hizb-ul-Mujahideen and Lashker-e-Toiba have a well-established network of OGWs which is sustaining militancy in Kashmir.

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

- **Operation All Out** by armed forces to eliminate the militant networks, their OGW, and top militant commanders.
- **Operation Sadbhavana (Goodwill)** by Indian Army in J&K to address aspirations of people affected by terrorism.
- **Mission Pehal** to encourage the youth to express their grievances against Indian state; the Army officers etc.
- **Education scholarships and livelihood schemes** such as USTTAD, Udaan, and Nai Manzil.
- **Training and employment opportunities for the youth** under many schemes such as HIMAYAT and **PMKVY**.
- **Other steps by Law enforcing agencies include**: sharing of intelligence inputs on real time basis, Tracking flow of funds to terrorist organisations by NIA etc.

### 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 so that the intelligence picture generated is in sync with ground realities.
- **Youth engagement programmes** (like Youth forums) should be widened to include addressing their sense of alienation and the trust deficit.
- Evolve a long-term and **multidisciplinary de-radicalization and counter-radicalization policy** for Kashmir.
- **Psychological and social rehabilitation** as well as strategic communication.
- **Investing in AI and other technologies** to discourage extremist content on social media.

### Conclusion

OGWs can constantly work towards the development of a negative sentiment in the minds of grey population or fence sitters in an insurgency.

There is a need to jointly map the OGWs, terrorists and anti-national elements through a multi-agency effort to create and plan strategies that are in sync with ground realities.

**Related News**

Kashmir valley has seen a **rise in the attacks being carried out by 'Part time or Hybrid terrorists'.**

- **About Hybrid terrorists**
  - They are **not listed with security forces** but are in touch with militants.
  - "Hybrid" militant can be a boy next door who **had been radicalised and kept on standby mode** by the handlers for carrying out a terror incident.
  - They **carry out a task** that is given to them and t**hen waits for the next assignment** from their masters. In between, they **go back to normal work.**
  - Such militants use **weapons like "pistols and grenades"** to create an atmosphere of "terror and fear".

- **Challenges posed by hybrid terrorism:**
    - While security forces track full-time terrorists or OGWs, there is **difficulty in identifying and tracking** the part-time or hybrid terrorists as they are engaged in their normal work.
    - It is difficult to **arrest them or stop them or neutralizing** them in encounters.
- Security forces are resorting to **use of technical gadgets and cyber patrol** to identify and track them.

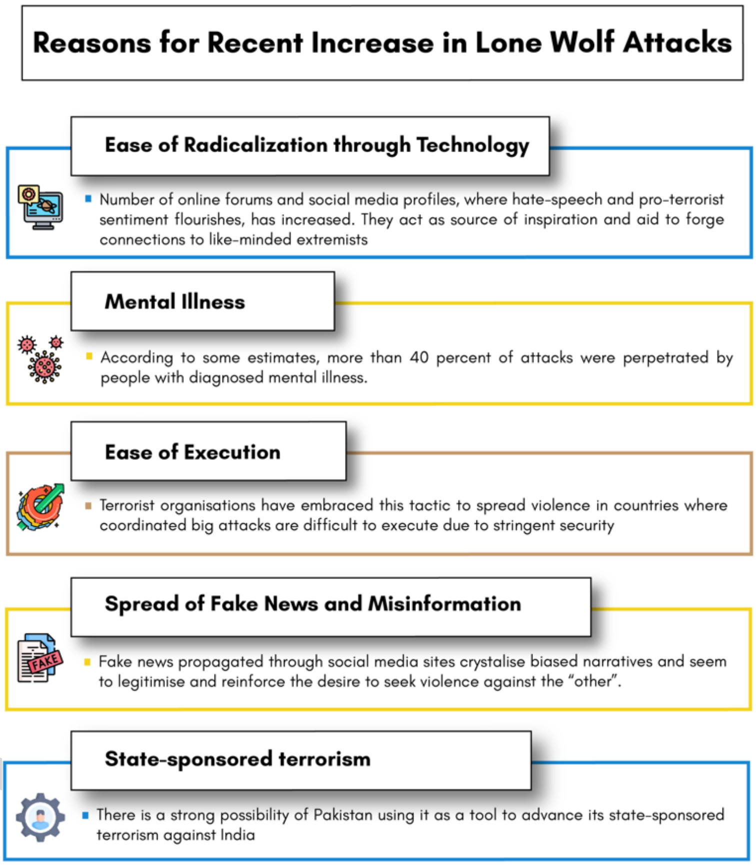
## 6.5. LONE WOLF ATTACKS

### Why in News?

Recent data shows that, because of a string of successful counter-insurgency operations, terrorists are increasingly resorting to lone-wolf attacks against security forces in Kashmir.

### About Lone wolf Attacks

- These attacks involve **threat or use of violence by a single perpetrator** (or a small cell).
- A lone wolf **acts without any direct support of any other group** or other individual in the planning, preparation and execution of the attack.
- Though lone wolf prefers to act totally alone, **his or her radicalization to action maybe spurred by violent media images,** incendiary books, manifestos, and fatwas.
- Ranging from **threatening and intimidating people** to indiscriminate shootings, vehicle ramming, stabbing and suicide bombings, lone wolf terror attacks have become a grave threat.



Reasons for Recent Increase in Lone Wolf Attacks

Ease of Radicalization through Technology

- Number of online forums and social media profiles, where hate-speech and pro-terrorist sentiment flourishes, has increased. They act as source of inspiration and aid to forge connections to like-minded extremists

Mental Illness

- According to some estimates, more than 40 percent of attacks were perpetrated by people with diagnosed mental illness.

Ease of Execution

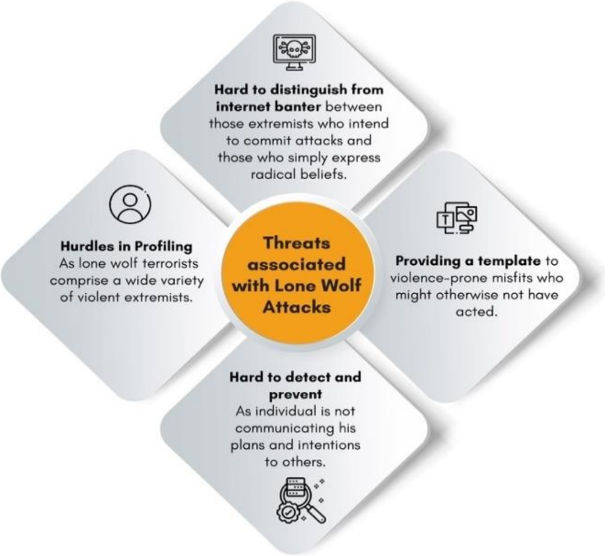
- Terrorist organisations have embraced this tactic to spread violence in countries where coordinated big attacks are difficult to execute due to stringent security

Spread of Fake News and Misinformation

- Fake news propagated through social media sites crystalise biased narratives and seem to legitimise and reinforce the desire to seek violence against the "other".

State-sponsored terrorism

- There is a strong possibility of Pakistan using it as a tool to advance its state-sponsored terrorism against India



Threats associated with Lone Wolf Attacks

**Hard to distinguish from internet banter** between those extremists who intend to commit attacks and those who simply express radical beliefs.

**Hurdles in Profiling** As lone wolf terrorists comprise a wide variety of violent extremists.

**Providing a template** to violence-prone misfits who might otherwise not have acted.

**Hard to detect and prevent** As individual is not communicating his plans and intentions to others.

### Way Forward

- A **multi-pronged approach towards radicalization** must be adopted anchored in human intelligence, strong ties with communities and community leaders and deradicalization programmes.
- **Monitoring social media** can help officials spot potential attackers without previous connections to other terrorists.
- Try to make lone-wolf attacks less lethal by **limiting access to explosive materials,** semiautomatic weapons etc.
- **Taking proactive measures** such as training and equipping the local police, contingency plans by the intelligence and counter-terrorism structures, and a robust national counter-terrorism doctrine.
- **Big data analytics can be used to discern the level of radicalization** of

**Steps taken by India**

- **Strict laws** have made gaining access to explosives, light weapons and other ammunitions in India immensely difficult.
- **India's cultural pluralism and democratic values** has helped counter extremist ideologies.
- India has the third largest Muslim population in the world, only a **minuscule fragment of the population has expressed interest in joining or sympathises with IS.**
- **Strong security apparatus** along with the reforms in the counter-terrorism structure in the aftermath of 2008 Mumbai terror attacks is a major deterrent.

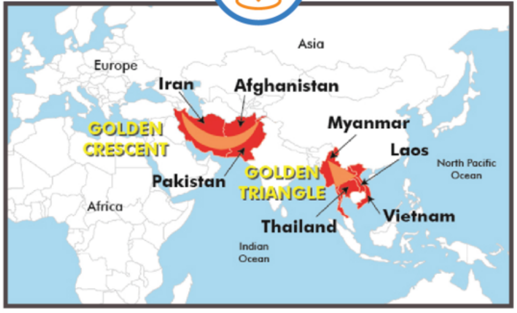
potential recruits, their networks and sources of information, funding and leadership in order to help unravel the roots of radicalization.

## 6.6. DRUG TRAFFICKING IN INDIA

# DRUG TRAFFICKING IN INDIA AT A GLANCE

Drug trafficking is a **global illicit trade involving the cultivation, manufacture, distribution, and sale of substances** which are subjected to drug prohibition laws.

**Reasons for heightened drug trafficking in India:** Increased production of opium in Afghanistan, greater domestic demand in India, favourable geographical location etc.



### Drug Trafficking characteristics in India

- As per the **United Nations Office on Drugs and Crime (UNODC)** report, **India is one of the world's single-largest opiate markets in terms of users** (World Drug Report 2022 **).**
- **India has become a transit hub as well as a destination** for heroin and hashish produced in Golden Triangle and Golden Crescent.
- Worst affected regions are North East India (especially Manipur) and North West India (especially Punjab) followed by Mumbai and Delhi and now Haryana.

### Drugs trade as significant threat to the national security

- **Facilitates other organised criminal** enterprises.
- **Destabilise nation by Narco-terrorism,** the nexus between drug traffickers, criminal networks and terrorists.
- Money generated by the illegal sale of narcotics and drugs is **used for financing terrorist activities** and also left-wing extremism.
- **Encourages drug consumption** thereby creating law and order problem in the society.
- Drug cartels **subvert, penetrate and further corrupt state institutions** to control the illegal drug trade.

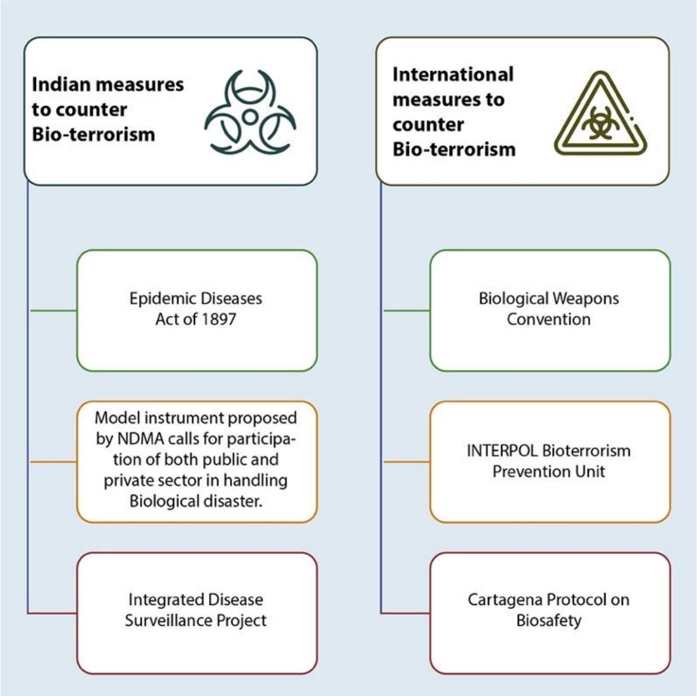
### Measures taken by India

- **Enacting legislations** such as Narcotics Drugs and Psychotropic Substances Act.
- **Ensuring physical security of the borders and coasts** by strengthening patrolling and surveillance.
- **India has signed several bilateral pacts** with different countries for combating illicit trafficking of narcotic, drugs and psychotropic substances.
- **Nasha Mukt Bharat Annual Action Plan (2020-21).**
- **Launched an e-portal called 'SIMS'** (Seizure Information Management System) for cases involving large seizures.
- **Co-operating with voluntary organisations and being signatory to various UN conventions:** namely, Single Convention on Narcotic Drugs, 1961, Convention on Psychotropic Substances, 1971 and Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988.

### Way Forward

- **Effective coordination and information sharing** among enforcement agencies.
- **Develop accountability mechanisms and practices** for shipping and railway companies, postal services, and air cargo.
- **Control the drug supply chain on the Internet** by regulating cryptocurrency markets and monitor electronic payment.
- **Enhancement of punishment** under NDPS and other drug laws.
- **Creating awareness among citizens** and establishing de-addiction centres and camps.

## 6.7. BIO-TERRORISM



Indian measures to counter Bio-terrorism

- Epidemic Diseases Act of 1897
- Model instrument proposed by NDMA calls for participation of both public and private sector in handling Biological disaster.
- Integrated Disease Surveillance Project

International measures to counter Bio-terrorism

- Biological Weapons Convention
- INTERPOL Bioterrorism Prevention Unit
- Cartagena Protocol on Biosafety

### Why in news?

Recently, United Nations (UN) declared that it is not aware of any biological weapons programmes in Ukraine amid Russia's claims that the US is funding "military biological activities" in Ukraine.

### About bio-terrorism

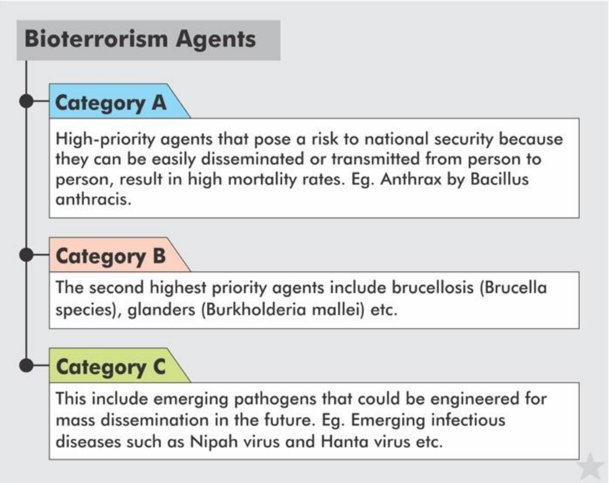
- **Bioterrorism is a planned and deliberate use of pathogenic strains of microorganisms** such as bacteria, viruses, or their toxins to spread life-threatening diseases on a mass scale in order to devastate the population of an area.
- These agents are **delivered by Scud missiles, motor vehicles with 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**: 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 biotechnology and nanotechnology** that has created an easy accessibility to more sophisticated biologic agents apart from the conventional bacteria, viruses and toxins.

### 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.
- **Prevention:** through examining the risk of bioterror attacks, preparation and training of law enforcement personnel, and the related legal and political framework for enhanced intelligence.
- **Surveillance and assessment**: by recognizing patterns of non-specific syndromes and assessing them, that could indicate the early manifestations of a biological warfare attack.
- **Laboratory investigation:** Need to develop both laboratory- and institution-wide response plans for diagnosis and characterization of the biological organism.
- **Medical management**: It should include preventive, promotive, and curative services like Chemoprevention to prevent the spread of the disease.
- **General public sensitization:** through training and education, warning network at hospitals and public health agencies etc.



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.

### Conclusion

Bio-terrorism is a long-term, continually evolving threat and India needs strong institutional and legal measures to prevent and mitigate different types of biological threats.

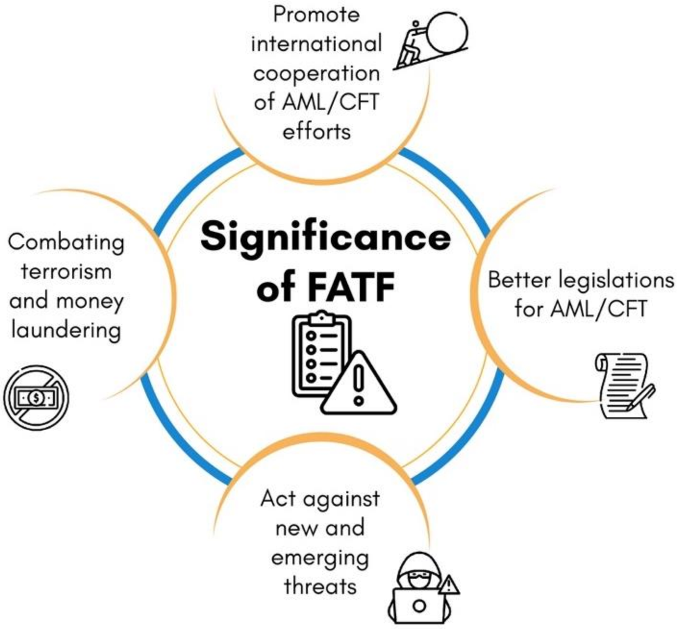
## 6.8. FINANCIAL ACTION TASK FORCE (FATF)

### Why in News?

Recently, the Finance Minister attended the FATF Ministerial Meeting and endorsed the FATF's strategic priorities for the years 2022-24.

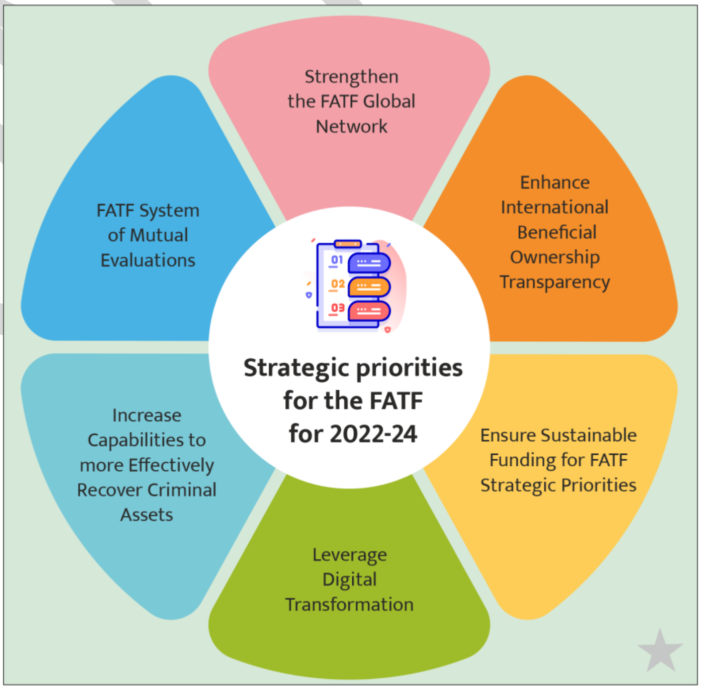
### About Financial Action Task Force (FATF)

- It is an **inter-governmental body** established in 1989 **to combat money laundering, terrorist financing, and other related threats** to the integrity of the international financial system.
- **FATF Recommendations are recognised** as the global **anti-money laundering (AML) and counter-terrorist financing (CFT) standard.**
  - FATF also works to stop **funding for weapons of mass destruction.**


Significance of FATF
Promote international cooperation of AML/CFT efforts
Better legislations for AML/CFT
Act against new and emerging threats
Combating terrorism and money laundering

### Challenges faced by FATF

- **Project interest of selected nations:** Critics believe that on behalf of the interests of a few select states (EU Member States, US) it imposes regulations that are illegitimate and costly.
- **Lack of transparency in working:** Meetings of the group are carried out behind closed doors, and deliberations are not publicised. FATF has also penalised countries that have disclosed the contents of its meetings.
- **Difficulty in domestic coordination:** because of challenges in reaching a mutual understanding of what the FATF recommendations mean and how a country should judge its performance relative to the recommendations.
- **Capacity constraints of countries:** This includes difficulties in investigating and prosecuting high-profile cross-border cases and preventing anonymous shell companies and trusts being used for illicit purposes
- **Operational challenges:** Inadequate, weak and selective enforcement of AML/CFT provisions, Ineffective penalties etc. are some of the reasons why the FATF strategy has not been more successful.
- **New-age Challenges:** including bitcoins and cyber currencies, illegal trafficking of wildlife as a source of funding, use of artificial intelligence in terror attacks and biowarfare have emerged.

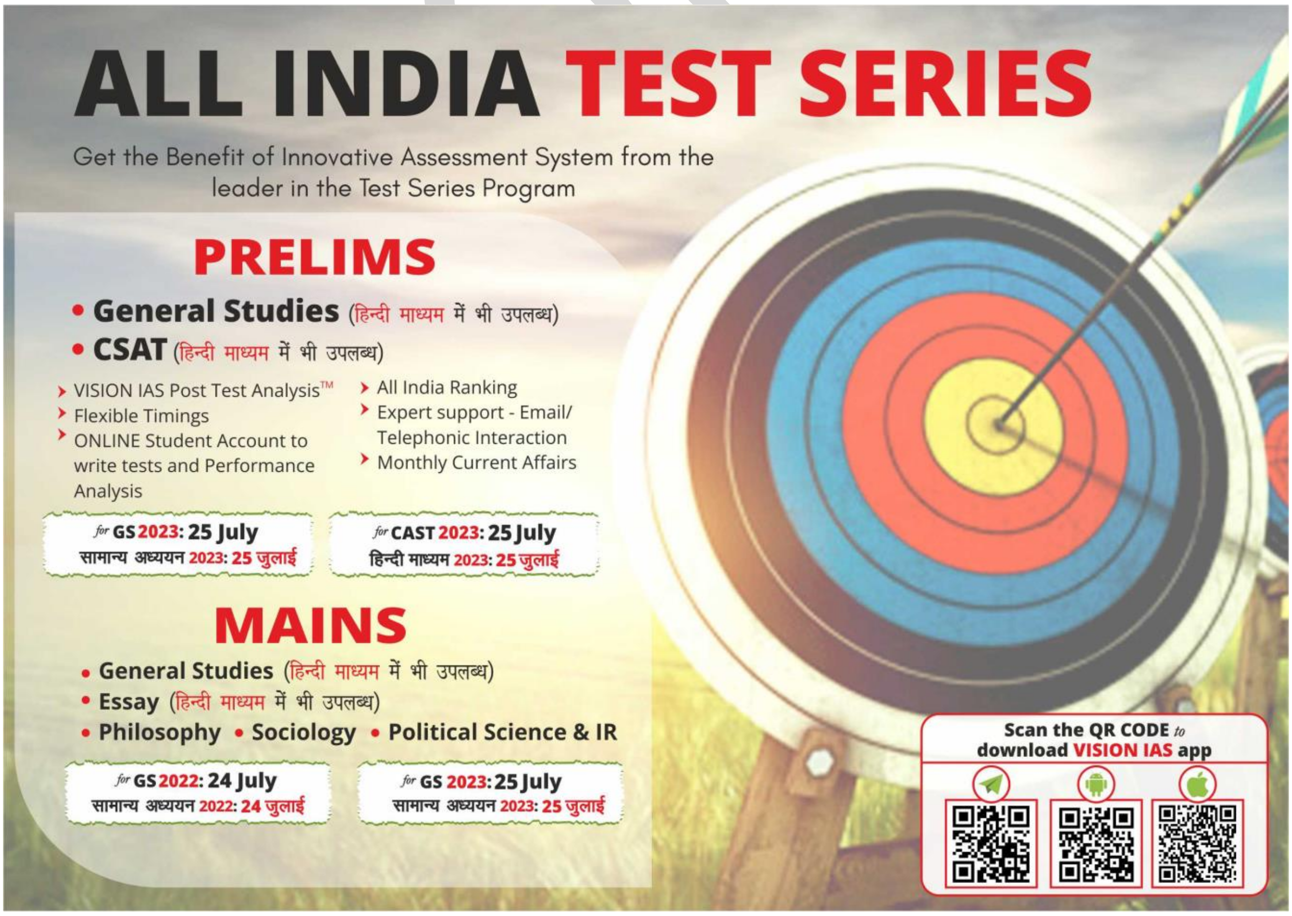

Strategic priorities for the FATF for 2022-24
Strengthen the FATF Global Network
Enhance International Beneficial Ownership Transparency
Ensure Sustainable Funding for FATF Strategic Priorities
Leverage Digital Transformation
Increase Capabilities to more Effectively Recover Criminal Assets
FATF System of Mutual Evaluations
01
02
03

**India's anti-money laundering and countering terrorist financing measures**

- Guidelines and rules framed under the **Prevention of Money Laundering Act (PMLA)**
- Strict **adherence to Know Your Customer (KYC)** procedures
- **Enactment of the Fugitive Economic Offenders Act** in 2018
- **Anti-black money Act of 2015**
- New compliance regime brought in by the **Financial Intelligence Unit (FIU) for banks, other financial institutions.**

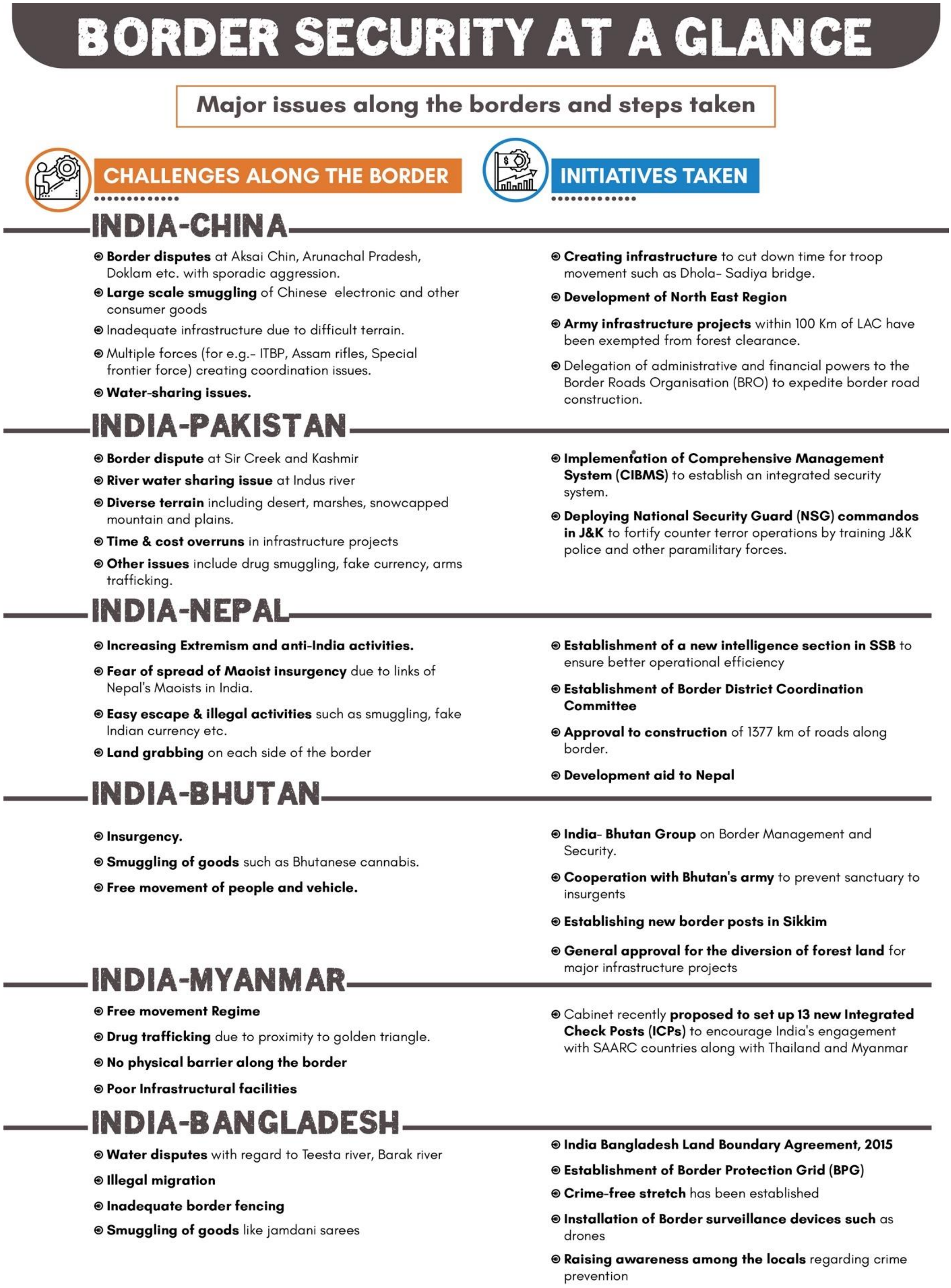
### Way Forward

- **Better regulatory framework:** to include non-financial sectors, ensuring adequate supervision and implementation of adequate, proportionate, and dissuasive sanctions when needed.
- **Improved international cooperation:** Countries should establish dedicated liaison officers overseas to facilitate exchanges and joint investigations into complex cases involving multiple jurisdictions.
- **Better Compliance mechanism:** Compliance with AML/CFT legislation requires a multi-layered and coordinated response from financial institutions and government.
- **Enhanced cooperation with private sector:** It will provide ability to better identification, understanding and management of money laundering, terror financing; greater auditability and accountability etc.
- **Adopting new technologies:** such as AI, Data analytics etc can improve the speed, quality and efficiency of measures to combat money laundering and terrorist financing.



# 7. BORDER SECURITY AND MANAGEMENT

## 7.1. BORDER MANAGEMENT



### BORDER SECURITY AT A GLANCE

Major issues along the borders and steps taken

CHALLENGES ALONG THE BORDER | INITIATIVES TAKEN

#### INDIA-CHINA

Challenges along the border:

- **Border disputes** at Aksai Chin, Arunachal Pradesh, Doklam etc. with sporadic aggression.
- **Large scale smuggling** of Chinese electronic and other consumer goods
- Inadequate infrastructure due to difficult terrain.
- Multiple forces (for e.g.- ITBP, Assam rifles, Special frontier force) creating coordination issues.
- **Water-sharing issues.**

Initiatives taken:

- **Creating infrastructure** to cut down time for troop movement such as Dhola- Sadiya bridge.
- **Development of North East Region**
- **Army infrastructure projects** within 100 Km of LAC have been exempted from forest clearance.
- Delegation of administrative and financial powers to the Border Roads Organisation (BRO) to expedite border road construction.

#### INDIA-PAKISTAN

Challenges along the border:

- **Border dispute** at Sir Creek and Kashmir
- **River water sharing issue** at Indus river
- **Diverse terrain** including desert, marshes, snowcapped mountain and plains.
- **Time & cost overruns** in infrastructure projects
- **Other issues** include drug smuggling, fake currency, arms trafficking.

Initiatives taken:

- **Implementation of Comprehensive Management System (CIBMS)** to establish an integrated security system.
- **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

Challenges along the border:

- **Increasing Extremism and anti-India activities.**
- **Fear of spread of Maoist insurgency** due to links of Nepal's Maoists in India.
- **Easy escape & illegal activities** such as smuggling, fake Indian currency etc.
- **Land grabbing** on each side of the border

Initiatives taken:

- **Establishment of a new intelligence section in SSB** to ensure better operational efficiency
- **Establishment of Border District Coordination Committee**
- **Approval to construction** of 1377 km of roads along border.
- **Development aid to Nepal**

#### INDIA-BHUTAN

Challenges along the border:

- **Insurgency.**
- **Smuggling of goods** such as Bhutanese cannabis.
- **Free movement of people and vehicle.**

Initiatives taken:

- **India- Bhutan Group** on Border Management and Security.
- **Cooperation with Bhutan's army** to prevent sanctuary to insurgents
- **Establishing new border posts in Sikkim**
- **General approval for the diversion of forest land** for major infrastructure projects

#### INDIA-MYANMAR

Challenges along the border:

- **Free movement Regime**
- **Drug trafficking** due to proximity to golden triangle.
- **No physical barrier along the border**
- **Poor Infrastructural facilities**

Initiatives taken:

- 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

Challenges along the border:

- **Water disputes** with regard to Teesta river, Barak river
- **Illegal migration**
- **Inadequate border fencing**
- **Smuggling of goods** like jamdani sarees

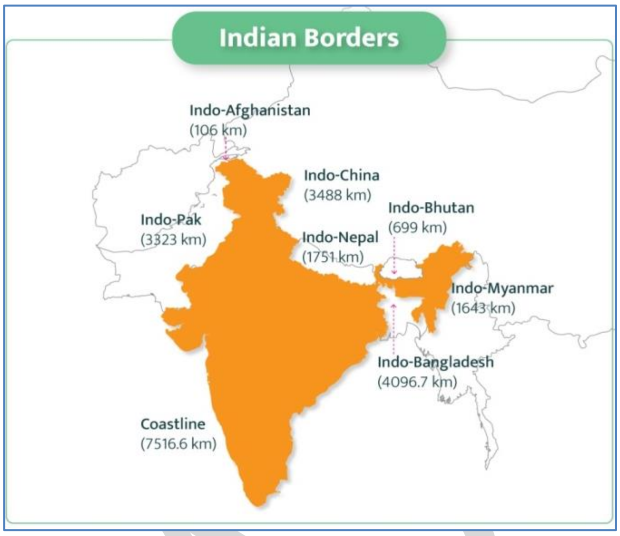
Initiatives taken:

- **India Bangladesh Land Boundary Agreement, 2015**
- **Establishment of Border Protection Grid (BPG)**
- **Crime-free stretch** has been established
- **Installation of Border surveillance devices such** as drones
- **Raising awareness among the locals** regarding crime prevention

## 7.2. POLICING POWER TO CENTRAL ARMED POLICE FORCES (CAPFS)

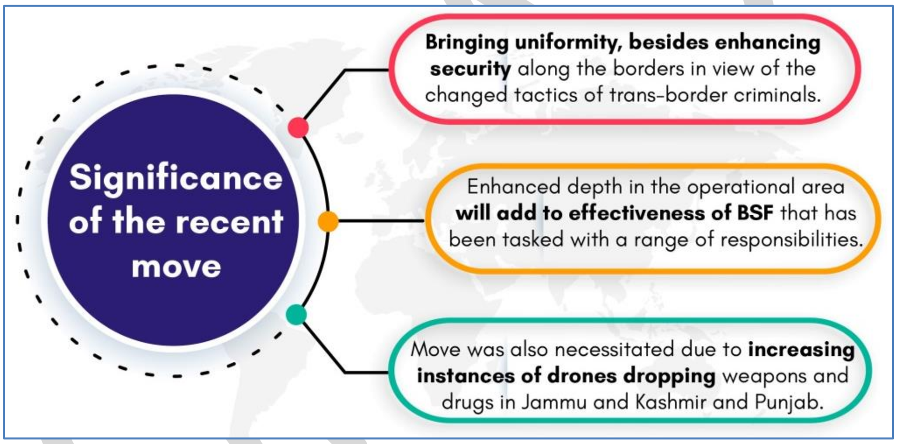
### Why in News?

Recently, Ministry of Home Affairs (MHA)'s notification set the **jurisdiction of the Border Security Force (BSF) at a uniform limit of 50 Km** in almost all the states that share borders with **Pakistan, Bangladesh and Myanmar**.



### More on News

- **Notification will enable the BSF** to prevent offences that fall under a variety of acts including the Criminal Procedure Code (CrPC), Passport (Entry into India) Act, 1920 and the Passport Act, 1967.
- The notification, however, **does not give the BSF the power to investigate crimes.** Suspects and accused persons will still have to be handed over to the local authorities.



**Significance of the recent move**

**Bringing uniformity, besides enhancing security** along the borders in view of the changed tactics of trans-border criminals.

Enhanced depth in the operational area **will add to effectiveness of BSF** that has been tasked with a range of responsibilities.

Move was also necessitated due to **increasing instances of drones dropping** weapons and drugs in Jammu and Kashmir and Punjab.

### Why was delegation of the power required?

- **Rising security threats:** State police forces alone are unable to tackle a host of unconventional security threats and challenges that India faces (terrorism, Left-Wing Extremism (LWE), and insurgency).
  - Challenges are faced because of the lack of advanced equipments and arms, inadequate training of personnel and the inability of the State Governments to modernize their police forces.
- **Limitation of state police:** There is an external dimension to the country's security scenario which limits the role of the state police forces and this necessitates the intervention of the Central Government
- **Policing of border areas:** BSF being the only law enforcing agency present in remote border areas in Gujarat and Rajasthan required that police powers delegated to the BSF be larger in these two states.
- **Enhancing effectiveness:** These powers enabled the forces to chase and apprehend trans-border criminals who may have managed to escape detection by BSF/SSB ambushes.
- **Other reasons:** These powers were considered essential in view of circumstances like the terrain, population composition, crime pattern besides presence and effectiveness of the police in border areas.

## Importance of Border States

### Role in Internal Security

Border regions and communities constitute India's first line of defence, a critical link in its national security.

### Role in Foreign Policy

- Border States can play important role in maximizing cross-border co-operation to promote social and economic development, through active encouragement from the Indian government.

### Enhancing Regional Cooperation

In this age of globalization and increased international cooperation, Border States also signify some new opportunities.

- Such opportunities are believed to be immense for Northeast India due to its geographical proximity to the prosperous East and Southeast Asian economies.

### Sub-Regional Integration

Border regions are beginning to effectively engage the Centre to deepen sub-regional integration processes.

- The effects of this lobbying can be seen in India's proposed decision to open 70 border haats long its border with Bangladesh.

**Issues arising from allocation of police powers to CAPFs**

- **Challenging Federalism:** as states argue that law and order is a state subject and enhancing BSF's jurisdiction infringes upon powers of the state government.
- **Lack of accessibility of National accountability mechanisms** than the regional accountability mechanisms offered by a state police force (the ability to walk into a local police station, for example).
- **Changed situation along borders:** Population density along with police presence in border areas has gone up in last 50 years. Enhancement of jurisdiction, therefore, may lead to confusion.
- **Core function of the BSF will get adversely affected**.
- **Lack of coordination with state police** may lead to ugly situations leading to turf wars, especially if the ruling parties in the state and centre are different.
- **Increased human rights violation:** increased jurisdiction of BSF, without adequate safeguards, might lead to arbitrary use of their powers and result in increased human rights violations.

**Conclusion**

A country of India's size and importance with **multiple porous and sensitive international borders** in a region as volatile as South Asia needs to be cautious about its border security.

But at the same time, as states in India's federal polity are entrusted with the primary responsibility of managing the law and order within its jurisdiction.

Enhancing police capacity and facilitating grounds for greater cooperation between CAPF and state police should be initiated jointly by the Centre and states.

**Related News**

**New Border Development Scheme to Focus on Making Model Villages**

- In recent budget, government announced **'vibrant village programme' to improve social and financial infrastructure in remote habitations,** primarily along the border with China.
  - Piloted by **MHA**, it is developed in the **backdrop of the Chinese setting up model villages** along India and Bhutan borders.
- The scheme would have **twin objectives of:**
  - Strengthening infrastructure along the border and
  - Ensuring that residents don't abandon their villages in search of economic opportunities in other areas.
- Activities will include **construction of village infrastructure, housing, tourist centres, road connectivity, direct-to-home access for Doordarshan and educational channel**s, and support for livelihood generation.
- **Need of the programme**:
  - Border villages with sparse population, limited connectivity and infrastructure often get **left out from development gains.**
  - To build "modern system of transportation and connectivity on the mountains" that will **help border villages of country to become vibrant.**
- **Other government steps to improve border villages:**
  - **Border Area Development Programme, launched in 1986-87** to meet developmental needs of people living in remote and inaccessible areas situated near the international border.
  - Union Budget 2022-23 has **increased capital outlay for Border Roads Organisation,** by a record 40 percent, as compared to FY 2021-22.

## 7.3. STRATEGIC IMPORTANCE OF ANDAMAN AND NICOBAR ISLANDS (ANI)

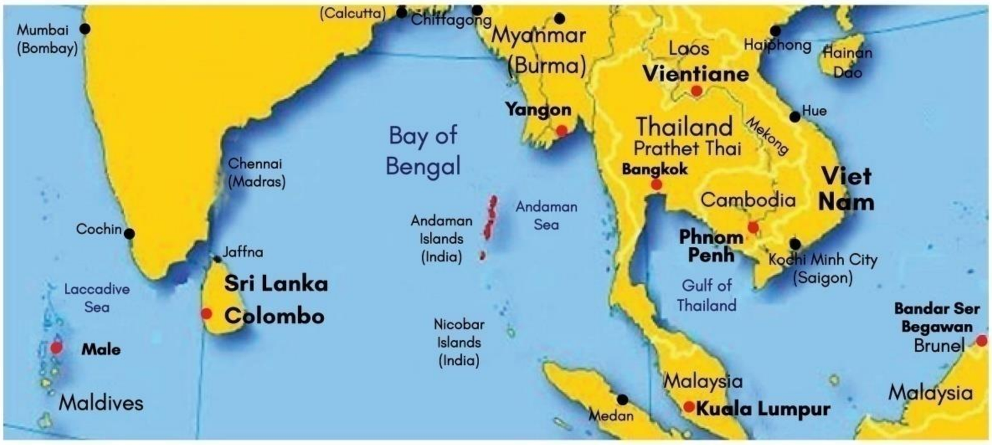
**Why in news?**

In the last few years, the **Andaman and Nicobar Islands (ANI)** have gained an important position in **India's foreign policy.**

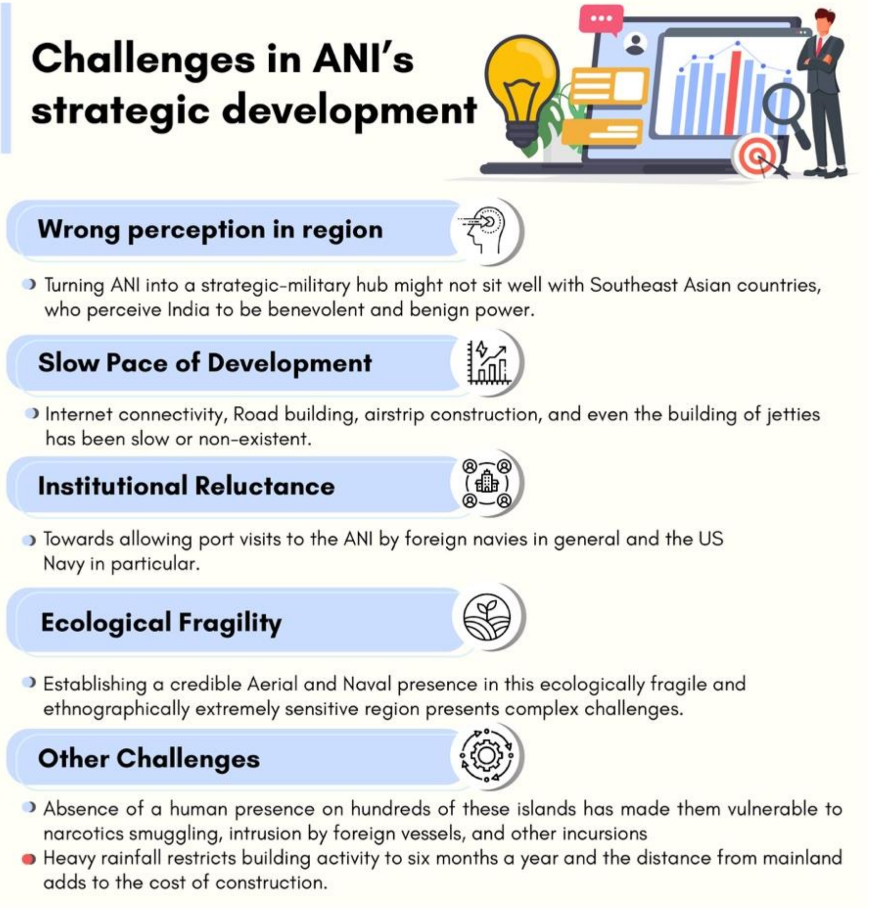
**Strategic importance of ANI**

- **Securing Sea Lines of Communications (SLOC)** by creating a series of chokepoints: **Preparis Channel** in the north, the **Ten Degree Channel** and the **Six Degree Channel** (used by vessels paasing through Malacca Strait) to the south.

- **Countering increasing Chinese presence:** By gaining ground at critical chokepoints, China could use them to **its benefit** during any **future conflict or a standoff with India**.
  - ANI's strategic location allows India to pursue **sea denial warfare** strategy to dictate terms in littoral space.



- **Net security provider:** India can also leverage the potential of these islands to protect its own interests and burnish its image as the 'net security provider' in the region.
- **Connection with Southeast Asia:** Containing about 30 percent of India's Exclusive Economic Zone (EEZ), ANI connects South Asia with Southeast Asia.
- **Important fulcrum of Indo-pacific:** The ANI are at the **intersection of the Indian Ocean and the South China Sea**, and further to the Pacific Ocean, an important fulcrum of the strategic concept of the Indo-Pacific.



## Challenges in ANI's strategic development

**Wrong perception in region**

- Turning ANI into a strategic-military hub might not sit well with Southeast Asian countries, who perceive India to be benevolent and benign power.

**Slow Pace of Development**

- Internet connectivity, Road building, airstrip construction, and even the building of jetties has been slow or non-existent.

**Institutional Reluctance**

- Towards allowing port visits to the ANI by foreign navies in general and the US Navy in particular.

**Ecological Fragility**

- Establishing a credible Aerial and Naval presence in this ecologically fragile and ethnographically extremely sensitive region presents complex challenges.

**Other Challenges**

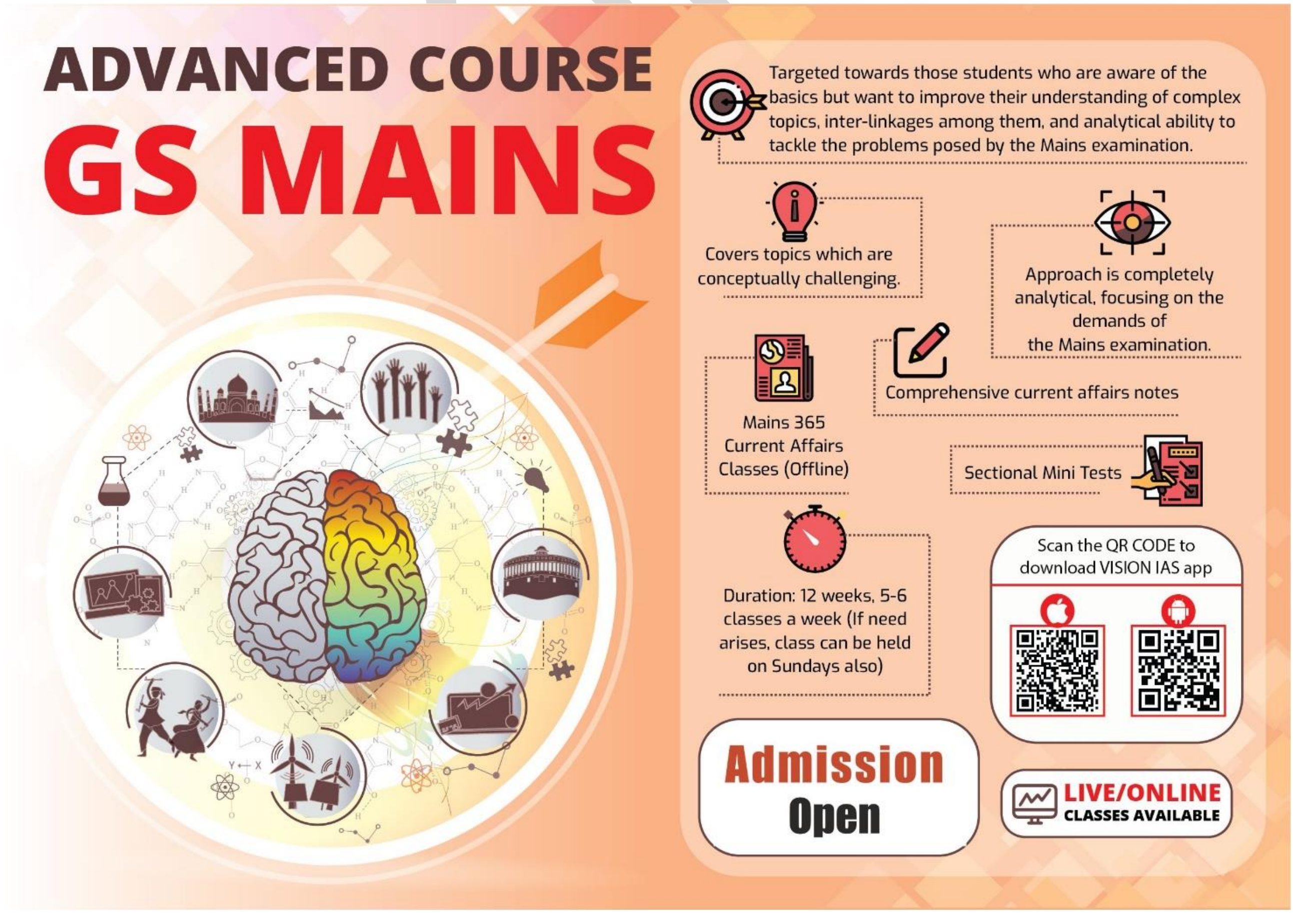
- Absence of a human presence on hundreds of these islands has made them vulnerable to narcotics smuggling, intrusion by foreign vessels, and other incursions
- Heavy rainfall restricts building activity to six months a year and the distance from mainland adds to the cost of construction.

**Initiatives taken in ANI**

- **Maritime hub:** In 2015, the government announced a plan to develop the islands into the country's first maritime hub to develop facilities, such as telecommunications, electricity, and water etc.
- **Declining protectionism:** In 2019, a new Island Coastal Regulation Zone Notification was promulgated, allowing land reclamation for ports, harbours and jetties. Allowing such projects will help in **creating strategic infrastructure.**
- **Maritime exercises**: Indian Navy conducts **joint maritime exercises** such as the Singapore India Maritime Bilateral Exercise, MILAN and Coordinated Patrols with Myanmar, Thailand and Indonesia..
- **Expanding naval presence**: Following the Ladakh stand-off with China in May 2020, India is expediting plans for **stationing additional forces, warships, aircraft, and missile batteries** in the ANI.
- **Others:**
  - The **Chennai-Andaman and Nicobar** undersea internet cable was inaugurated to provide **high-speed internet connection** to seven remote islands of the ANI chain.
  - In 2018, India and Indonesia set up a special task force to **enhance connectivity between the ANI and the port of Sabang** in Aceh to promote **trade, tourism and people-to-people contacts.**

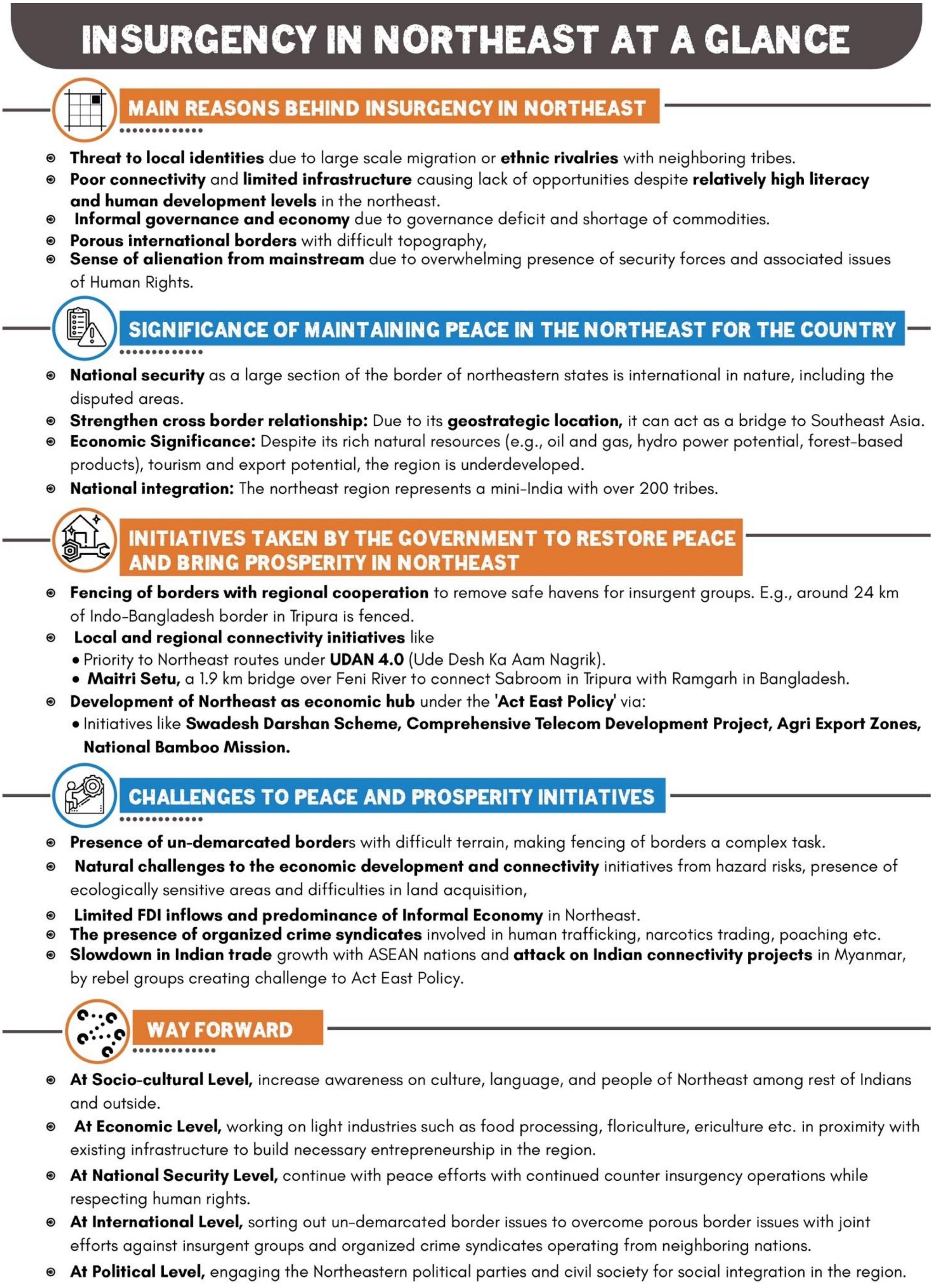
Road Ahead

- **Encouraging migration:** There is a need to consider encouraging migration from the mainland and open up some of the strategically located uninhabited islands to tourism.
- **Strategic infrastructure:** In a bid to emphasise its regional pre-eminence, the Indian Navy in recent times has raised the tempo of naval operations in the Bay of Bengal highlighting India’s combat prowess.
- **Cooperation with strategic partners: Port visits** by US, Japan, Australia, France or the UK can lead to further graded cooperation in all the dimensions.
- **Engagement with ASEAN:** There lies an opportunity to make ANI an important element of “Act East Policy” of engaging with countries in the region east of India.



Mains 365 - Security

# 8. INSURGENCY IN NORTHEAST



## 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.

### INITIATIVES TAKEN BY THE GOVERNMENT TO RESTORE PEACE AND BRING PROSPERITY IN NORTHEAST

- **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).
  - **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:
  - Initiatives like **Swadesh Darshan Scheme, Comprehensive Telecom Development Project, Agri Export Zones, National Bamboo Mission.**

### CHALLENGES TO PEACE AND PROSPERITY INITIATIVES

- **Presence of un-demarcated border**s 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.

### 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, ericulture 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.

## 8.1. BODO PEACE ACCORD

**Why in News?**

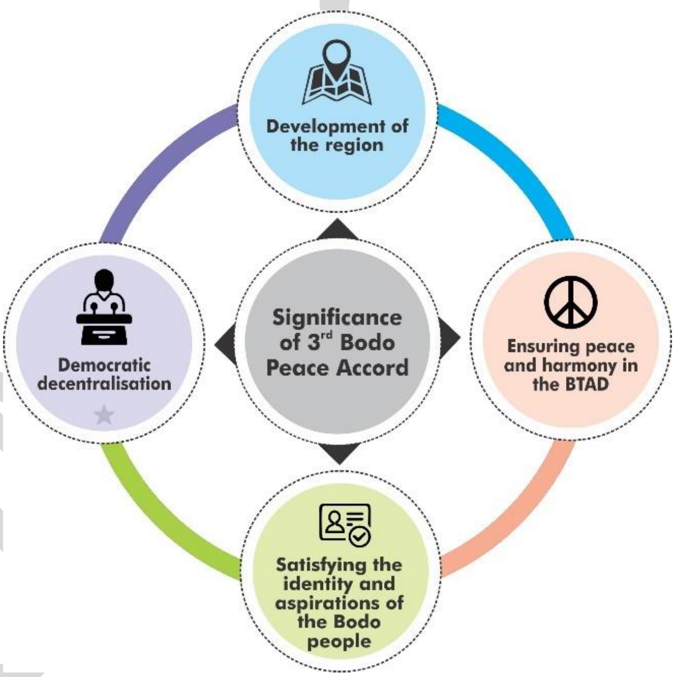
Recently, Prime Minister lauded the Bodo Accord, calling it the source of "long-lasting peace" in Assam.

**Timeline of the Bodoland dispute**

- **1960s and 1970s** - There were calls for a separate state of 'Udayachal', raised under the banner of the Plains Tribals Council of Assam (PTCA), a political outfit.
- **1993 - First accord was signed with All-Bodo Students Union (ABSU) that** led to the creation of Bodoland Autonomous Council (BAC) However, BAC failed.
- **2003** - **Second accord was signed with the Bodo Liberation Tigers** (BLT), and led to the formation of BTC, which included several districts (collectively called BTAD). BLT is disbanded.
- **2005** – NDFB agreed to a ceasefire. Later, it split into three factions. One of those factions, NDFB (S) continued to carry out violent attacks.

**About 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.
    - **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, **by the central government for the demarcation and reorganisation of the BTR.**
    - Bodos living in hills districts of KarbiAnglong and Dima Hasao would **be conferred Scheduled Hill Tribe status.**
    - **Number of seats in Bodoland Territorial Council (BTC) 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 was provided.


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

**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.
- More than 1,615 **cadres of NDFB laid down arms** and **assistance of Rs. 4 lakh** has been started **for all surrendered militants.**

**Related News**

A tripartite agreement among **five insurgent groups of Assam, the Centre and the State government** was signed to end years of violence in the Karbi Anglong region.

**Key highlights of the deal**

- **Rehabilitation** of more than 1,000 armed cadres have abjured violence and joined the mainstream.
- Centre will make available a **special development package of ₹1,000 crore over the next five years,** for the Assam government to undertake specific projects **for the development of Karbi areas.**

- **Greater devolution of autonomy to the Karbi Anglong Autonomous Council (KAAC),** protection of identity, language and culture of the Karbi people and focused development of the Council area, without affecting the territorial and administrative integrity of Assam, said the government**.**

## 8.2. NAGA PEACE TALKS

### Why in News?

Government entered into Ceasefire Agreement with National Socialist Council of Nagaland (K) Niki Group.

### More on News

- The agreement will be **in effect for one year** beginning September 8 and **more than 200 cadres of the group have surrendered** as part of the peace process.
- Government had already signed a **framework agreement with NSCN-IM under Framework Agreement for Naga Peace Accord) in 2015.**
  - Ceasefire agreements with other Naga groups namely, **NSCN-NK, NSCN-R and NSCN-K-Khango (breakaway factions of dominant groups NSCN-IM and NSCN-K** ) were also in place.

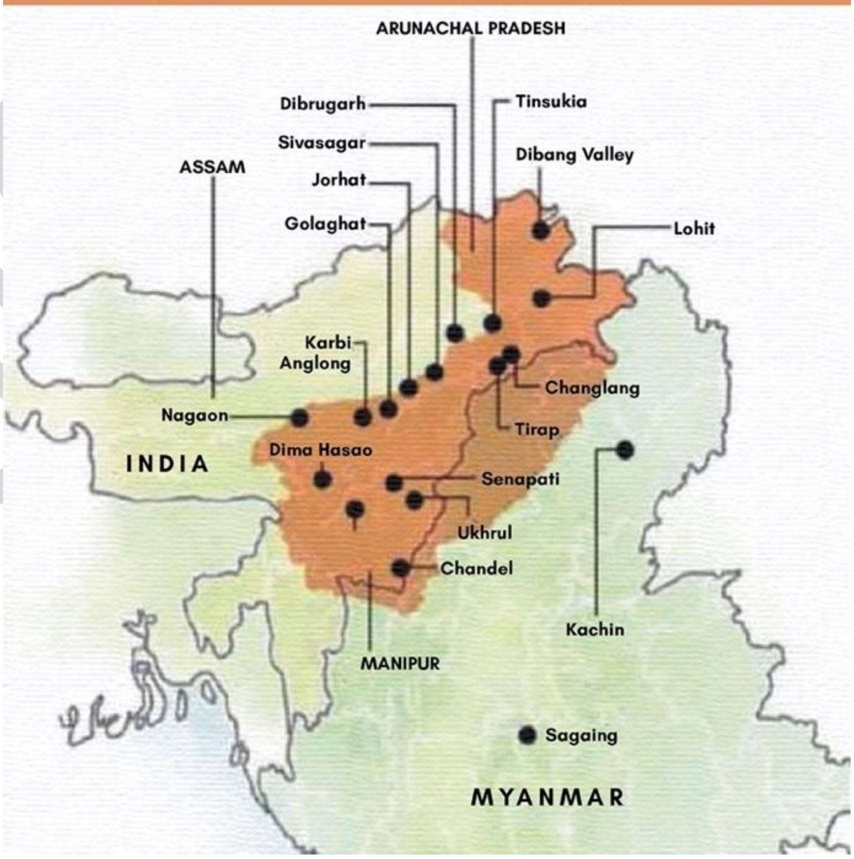
**About Naga movement**

- It is considered **India's longest-running insurgency**.
  - In **1946**, **AngamiPhizo** created **Naga National Council (NNC)** which declared Nagaland an Independent State on **14 August 1947.**
  - In **1975 NNC** agreed to give up violence under **Shillong Accord**, some leaders opposed it and in 1980 **National Socialist Council of Nagaland (NSCN)** emerged with demand for **Nagalim**, i.e. **Greater Nagaland.**
    - ✓ **Nagalim** comprising "all contiguous Naga-inhabited areas", which includes **Nagaland, several districts of Assam, Arunachal and Manipur, as also a large tract of Myanmar.**
- ○ The Nagas are **not a single tribe, but an ethnic community** that comprises several tribes who live in the state of Nagaland and its neighbourhood.

### Roadblock to Naga Peace talks

- **Nature of demand:** It is considered that the flag and constitution issue is integral to the core issues of the process and, therefore, a final settlement cannot be reached without these.
  - This requires fundamental changes in the country's federal dynamics.
- **Existence of Article 371A:** An amendment to this Article is critical to the ongoing Naga peace process in order to resolve another substantive issue of settling the question whether Nagas have the right over land and resources.
- **Integrity of other states:** It seems difficult that three states i.e., Manipur, Assam and Arunachal Pradesh would allow their territories to become a part of the 'Greater Nagalim.

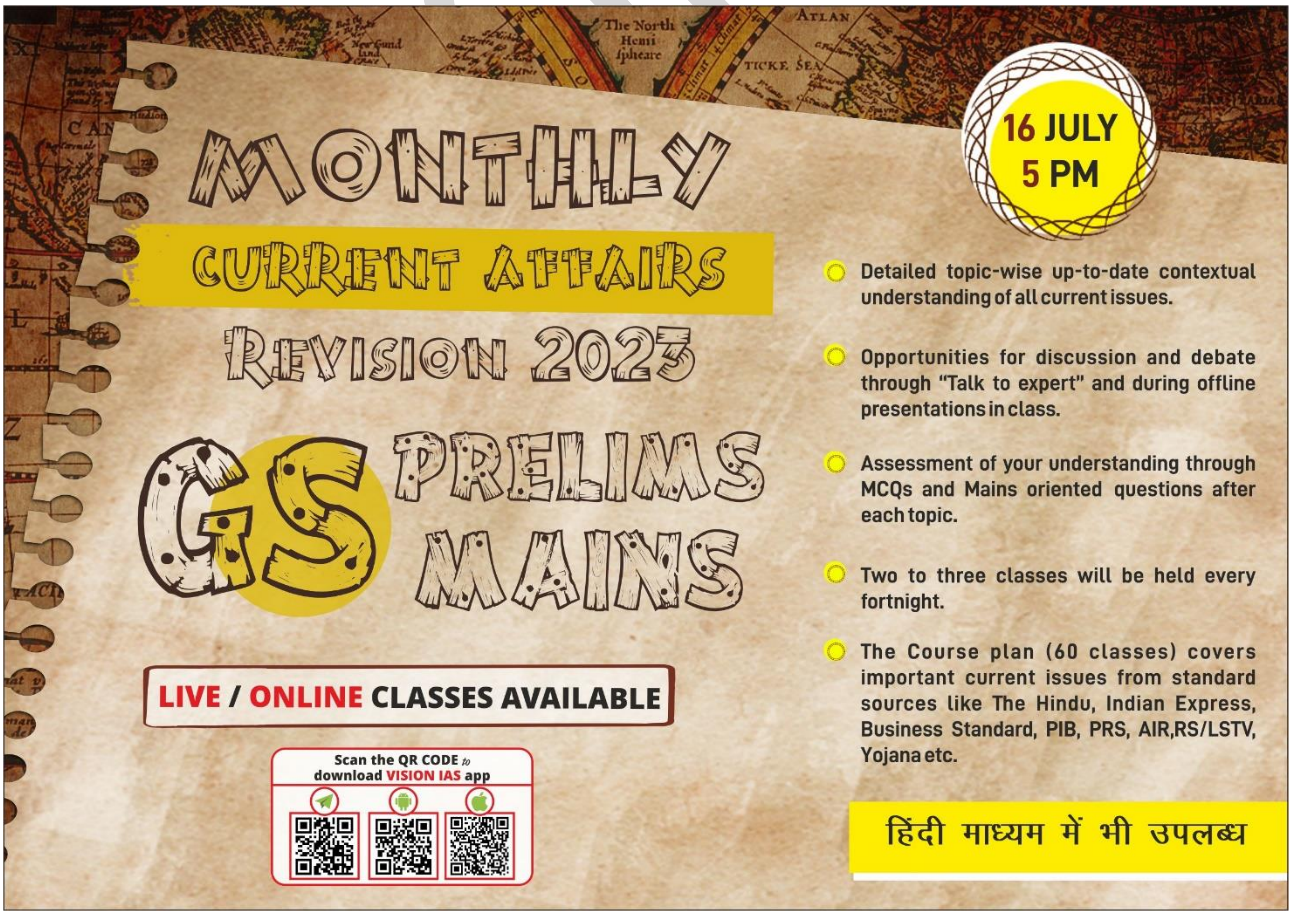
'GREATER NAGALIM', AS THE NSCN (IM) ORIGINALLY SOUGHT



- **Similar demand from other groups:** For instance, the Kuki groups, also in talks with the government, fear the Naga solution would carve up their imagined homeland.
- **Other reasons:** The situation and the negotiations get further complicated due to continued violence in the region, continuance of Armed Forces (Special Powers) Act and People losing faith in the overall management of the conflict

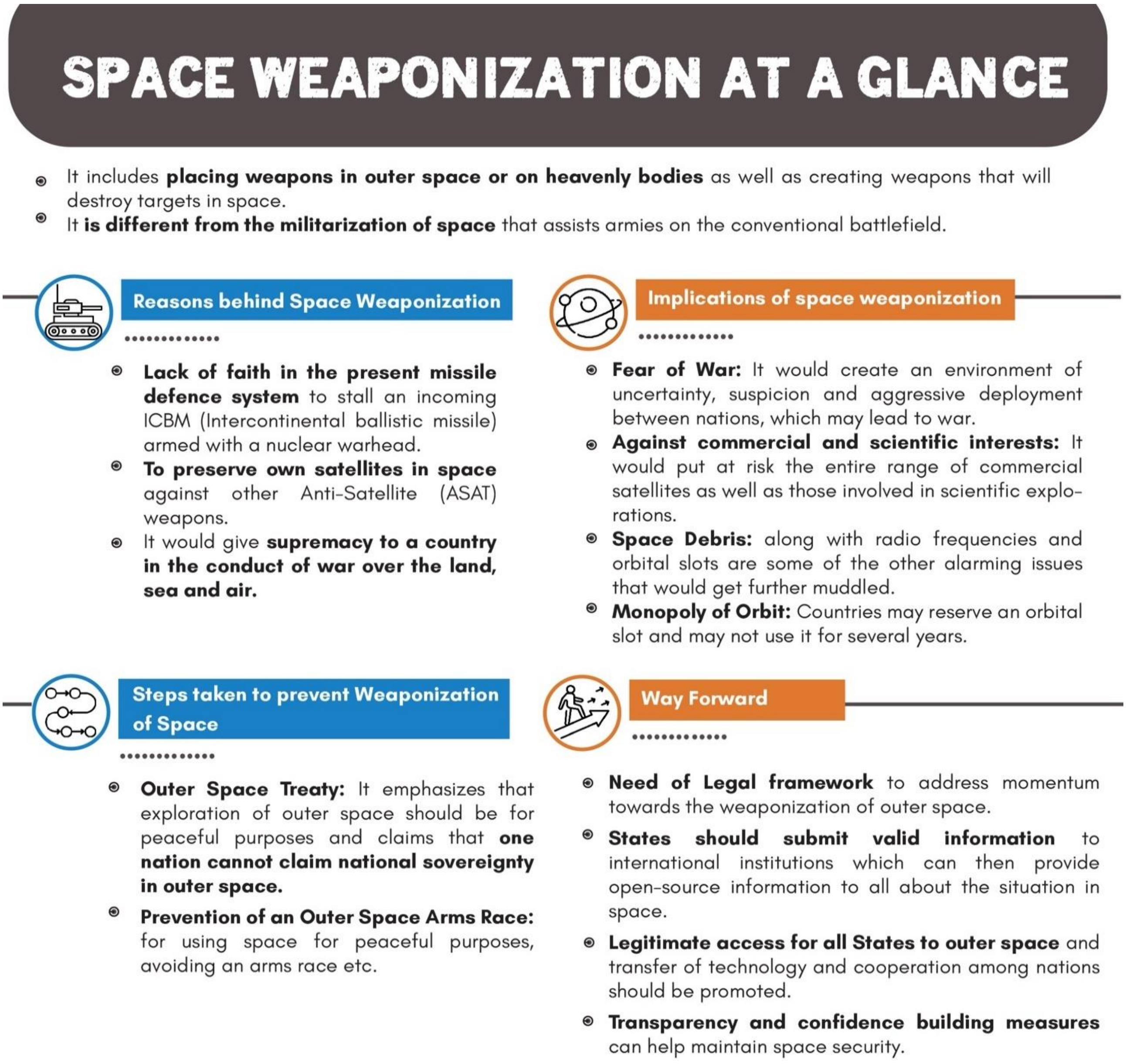
**Way forward**

- Government should **address the confusion due to many interpretations to "special arrangement"** implied in the 2015 agreement, particularly on how the shared sovereignty will be exercised.
- Government should not rush into declaring deadlines and **should involve all stakeholders from within and outside the state of Nagaland,** and work towards a solution through a peaceful dialogue process that satisfies all.
- **Other sections' sensitivities also will have to be kept in mind.** For example, Kukis, a tribe engaged in tussle with the Nagas in the Manipur hills, have to be politically assuaged.
- As Arunachal Pradesh, Assam and Manipur are wary of the NSCN-IM's concept of Nagalim, **government must take into confidence all genuine political formations,** civil society and ethnic groups.
- **People-to-people contacts need to be built up** so that real problems of the people can be voiced on a larger platform.



# 9. EMERGING DIMENSIONS OF SECURITY

## 9.1. SPACE WEAPONISATION



### SPACE WEAPONIZATION AT A GLANCE

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

**Reasons behind Space Weaponization**

- **Lack of faith in the present missile defence system** to stall an incoming ICBM (Intercontinental ballistic missile) armed with a nuclear warhead.
- **To preserve own satellites in space** against other Anti-Satellite (ASAT) weapons.
- It would give **supremacy to a country in the conduct of war over the land, sea and air.**

**Implications of space weaponization**

- **Fear of War:** It would create an environment of uncertainty, suspicion and aggressive deployment between nations, which may lead to war.
- **Against commercial and scientific interests:** It would put at risk the entire range of commercial satellites as well as those involved in scientific explorations.
- **Space Debris:** along with radio frequencies and orbital slots are some of the other alarming issues that would get further muddled.
- **Monopoly of Orbit:** Countries may reserve an orbital slot and may not use it for several years.

**Steps taken to prevent Weaponization of Space**

- **Outer Space Treaty:** It emphasizes that exploration of outer space should be for peaceful purposes and claims that **one nation cannot claim national sovereignty in outer space.**
- **Prevention of an Outer Space Arms Race:** for using space for peaceful purposes, avoiding an arms race etc.

**Way Forward**

- **Need of Legal framework** to address momentum towards the weaponization of outer space.
- **States should submit valid information** to international institutions which can then provide open-source information to all about the situation in space.
- **Legitimate access for all States to outer space** and transfer of technology and cooperation among nations should be promoted.
- **Transparency and confidence building measures** can help maintain space security.

## 9.2. EMERGING TECHNOLOGIES AND THREAT TO NATIONAL SECURITY

**Why in News?**

Recently, Union Home Minister said that **indigenously made anti-drone technology would soon be available** to tackle the challenges faced by drones in areas bordering Pakistan.

> **Emerging Technologies**
>
> - It commonly refers to **technologies that are currently developing, or that are expected to be available within the next five to ten years**, and is usually reserved for technologies that are creating, or are expected to create, significant social or economic effects.

**More on News**

- As drones from Pakistan continue to pose a threat in the border areas, the **country's security agencies have been discussing measures to deal with the arising situation.**

**Technology and Security**

- **Leadership in technological innovation** historically has been a **crucial national security asset** for major global powers.

Mains 365 - Security

- **Development and introduction of weapons** such as modern small arms, nuclear weapons, stealth technology, and guided missiles **altered the security equation** and, in some instances, transformed international relations.

| Emerging Technology | Possible Benefits | Possible Threat |
|---|---|---|
| Drones/ Unmanned aerial vehicles (UAV) | • UAVs have been used extensively for various purposes like **aerial photography and filmmaking, rescue operations, wildfire mapping,** crowd monitoring, etc. | • UAV could be used to **conduct reconnaissance, to spoof, distract or desensitize security forces.** |
| Remotely operated weapons systems (ROWS) | • **Enhanced Surveillance** (chemical and bio detection sensors, drones etc.) | • **Cyber infiltrators could gain access to control systems** and change the parameters of who is allowed in a given area and who is considered a threat thereby facilitate theft or sabotage. |
| Artificial intelligence (AI) | • **Counter terrorism and law enforcement** informatics via predictive analytics and AI. | • Automated, AI powered cyberattacks; risk of over-reliance on and over-complication of these systems; possibility that **terrorists and other adversaries will employ AI to help them plan and conduct more efficient physical attacks etc.** |
| Cyber Technology | • **Enhanced security** at nuclear power facilities and other complex industrial sites | • Increased risk of **hacking, disruption, and potential for sabotage** of critical infrastructure. |
| Enhanced Human Performance | • Includes a wide variety of focus, memory and emotion manipulating neuropharmaceuticals (nootropics), **physical performance-enhancing drugs** etc. | • This might enable new ways to **covertly perform reconnaissance, interface with computer systems** or communicate with collaborators. |
| Increasing use of outer space for defence and security | • Plays a **role in States' intelligence; surveillance and reconnaissance; troop movement tracking on land,** at sea, and in the air; classified and unclassified telecommunications; GPS-guided weapons; cyber-warfare etc. | • Expected introduction of directed energy weapons (DEW) and **possible increase in the military exploitation of satellite systems** for combat purposes. |

### Changing face of National security due to Emerging Technologies

- **Newer Threats:** New technologies and novel applications of existing technologies have the potential to disrupt labor markets and alter health, energy, and transportation systems.
- **Limited regulation:** In many cases, the rate of innovation is outpacing states' ability to keep abreast of the latest developments and their potential societal impacts.
- **Powerful adversaries:** Emerging technology will also allow our adversaries to strike farther, faster, and harder and challenge India in all warfare domains, including space.
- **Threat from Non-state actors:** Groups such as al-Qaeda and ISIS used online communication on Facebook, Twitter, YouTube, and other platforms to increase their prominence and recruit collaborators.
- **Threat of weapons of mass destruction (WMD):** Hostile nations, realizing that they cannot stand up to technologically superior military forces, will be stimulated to develop WMD as an offset to these capabilities.

**Steps taken by India**

- Ministry of External Affairs recently (MEA) created a **New, Emerging and Strategic Technologies (NEST) division** to deal with the foreign policy and international legal aspects of new and emerging technologies.
- **National Mission on Quantum Technologies & Applications** .
- **DRDO has also established several dedicated laboratories focusing on futuristic technologies** such as artificial intelligence, quantum and cognitive technologies, asymmetric technologies and smart materials.
- India has a **Defence Cyber Agency and a National Technical Research Organisation,** which are responsible for mechanisms that work to counter cyber risks and threats to the country.

### Way forward

- **Incentivizing investors and corporations** to consider national security in their decision-making process.
- **Multilateral governance system** to initiate, shape, and implement both technical and normative solutions.

- **More partnerships and collaborative environments** to share worldwide emerging technology trends, address competitive threats, share national security concerns, and consider civil liberties, privacy, and ethical implications.
- **Forming strategic public-private partnerships** with the aim of allocating private capital to support national security objectives.
- **Develop and adopt advanced technology applications** within government and improve the desirability of the government as a customer of the private sector.

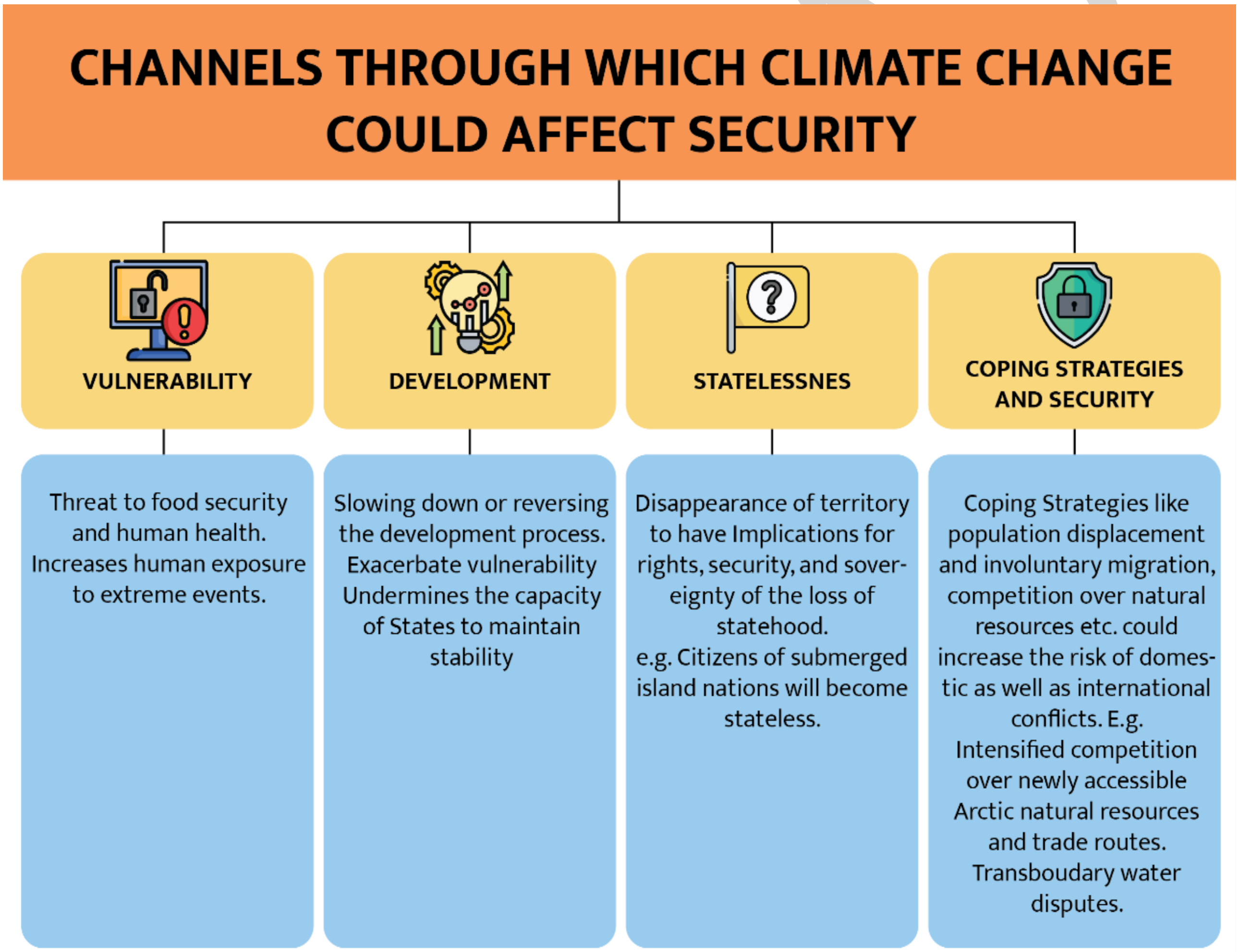
## 9.3. CLIMATE CHANGE AND SECURITY

### Why in News?

India voted against a United Nations Security Council (UNSC) draft resolution that for the first time would have defined climate change as a threat to peace.

### More on the news

- UNSC draft resolution was aimed at **systematically integrating climate-related security risks into the UN's conflict prevention, conflict management and peacebuilding work.**



**CHANNELS THROUGH WHICH CLIMATE CHANGE COULD AFFECT SECURITY**

**VULNERABILITY**

Threat to food security and human health. Increases human exposure to extreme events.

**DEVELOPMENT**

Slowing down or reversing the development process. Exacerbate vulnerability Undermines the capacity of States to maintain stability

**STATELESSNES**

Disappearance of territory to have Implications for rights, security, and sovereignty of the loss of statehood. e.g. Citizens of submerged island nations will become stateless.

**COPING STRATEGIES AND SECURITY**

Coping Strategies like population displacement and involuntary migration, competition over natural resources etc. could increase the risk of domestic as well as international conflicts. E.g. Intensified competition over newly accessible Arctic natural resources and trade routes. Transboudary water disputes.

### Need of the resolution

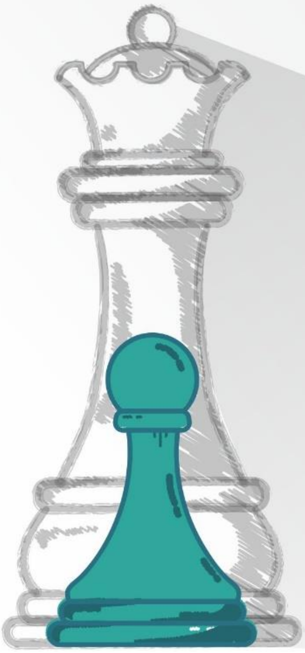
- **Interlinkage between Climate change and security** (refer infographic).
- **Progress of UNFCCC conferences is slow** and outcomes are inadequate to tackle climate change and associated challenges.
- **UNSC already has tools to address climate change within its mandate:** It can ensure that the security impacts of climate change are integrated into the critical work of peacekeeping, peacebuilding and humanitarian response.

**Concerns regarding resolution**

- While climate change has the potential to impact peace and security, the **nexus between the two is complex.**
  - For instance, other factors such as environmental degradation, food shortages and unfair distribution of resources are most likely to lead to tension and conflict.
- **Climate change lies outside the ambit of UNSC:** UNSC's primary responsibility is "maintenance of international peace and security" and all matters related to climate change are being discussed in UNFCCC, a specialised agency.
- **More powers to the world's industrialised countries,** which hold a veto power, to decide on future action on climate-related security issues, unlike UNFCCC, where decisions are made by consensus.

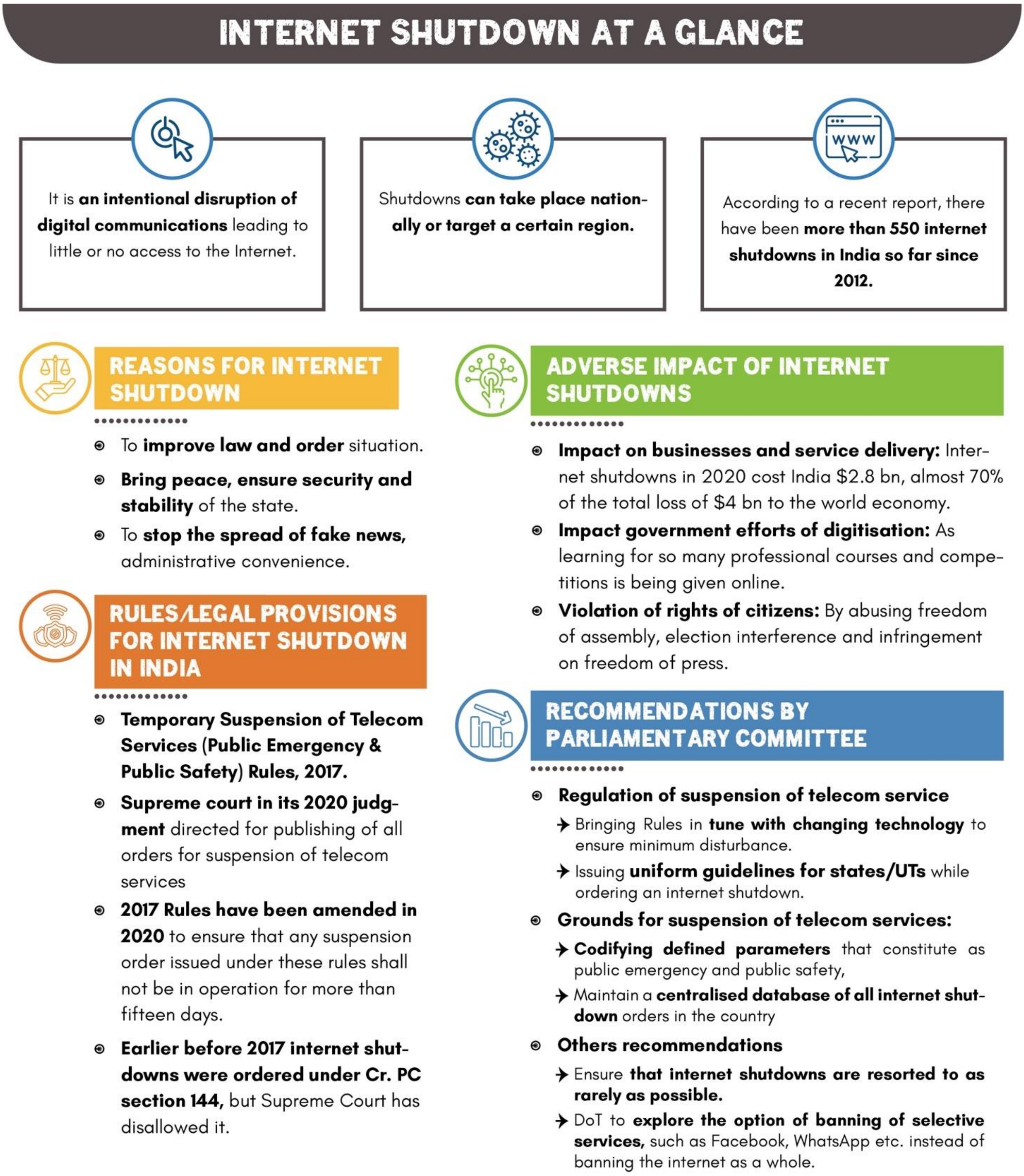
**Way forward**

- **UNFCCC can expand the scope of discussions** to include climate-related security issues.
- **International community must provide stronger support to climate change adaptation** in developing countries, including through investments in capacity-building at all levels.
- **Enhance global efforts to ensure the sustainable and equitable development of all countries**, notably through developed countries' meeting their international commitments on development assistance.
- **Anticipate and prepare to address unprecedented challenges** like possibility of large numbers of persons displaced across borders by climate change, prospect of statelessness of citizens of submerged island nations, drastic reduction in water availability etc.
- **Improve the flow of information and sharing of assessments**, particularly on early warning, between different regional and international organizations.



# 10. MISCELLANEOUS

## 10.1. INTERNET SHUTDOWN



### INTERNET SHUTDOWN AT A GLANCE

It is **an intentional disruption of digital communications** leading to little or no access to the Internet.

Shutdowns **can take place nationally or target a certain region.**

According to a recent report, there have been **more than 550 internet shutdowns in India so far since 2012.**

### REASONS FOR INTERNET SHUTDOWN

- To **improve law and order** situation.
- **Bring peace, ensure security and stability** of the state.
- To **stop the spread of fake news,** administrative convenience.

### RULES/LEGAL PROVISIONS FOR INTERNET SHUTDOWN IN INDIA

- **Temporary Suspension of Telecom Services (Public Emergency & Public Safety) Rules, 2017.**
- **Supreme court in its 2020 judgment** directed for publishing of all orders for suspension of telecom services
- **2017 Rules have been amended in 2020** to ensure that any suspension order issued under these rules shall not be in operation for more than fifteen days.
- **Earlier before 2017 internet shutdowns were ordered under Cr. PC section 144,** but Supreme Court has disallowed it.

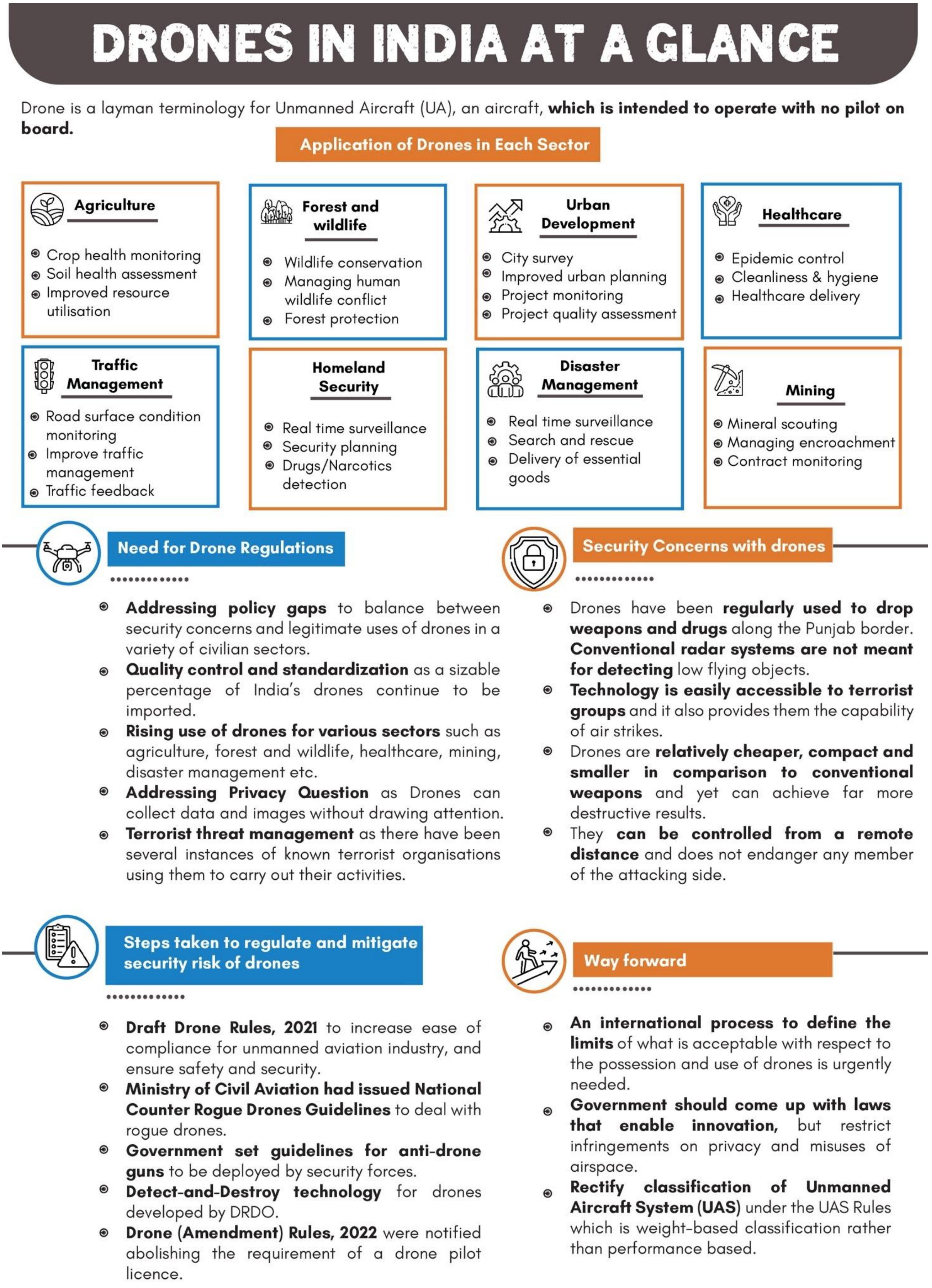
### ADVERSE IMPACT OF INTERNET SHUTDOWNS

- **Impact on businesses and service delivery:** Internet shutdowns in 2020 cost India $2.8 bn, almost 70% of the total loss of $4 bn to the world economy.
- **Impact government efforts of digitisation:** As learning for so many professional courses and competitions is being given online.
- **Violation of rights of citizens:** By abusing freedom of assembly, election interference and infringement on freedom of press.

### RECOMMENDATIONS BY PARLIAMENTARY COMMITTEE

- **Regulation of suspension of telecom service**
  - Bringing Rules in **tune with changing technology** to ensure minimum disturbance.
  - Issuing **uniform guidelines for states/UTs** while ordering an internet shutdown.
- **Grounds for suspension of telecom services:**
  - **Codifying defined parameters** that constitute as public emergency and public safety,
  - Maintain a **centralised database of all internet shutdown** orders in the country
- **Others recommendations**
  - Ensure **that internet shutdowns are resorted to as rarely as possible.**
  - DoT to **explore the option of banning of selective services,** such as Facebook, WhatsApp etc. instead of banning the internet as a whole.

## 10.2. DRONE REGULATIONS IN INDIA



# DRONES IN INDIA AT A GLANCE

Drone is a layman terminology for Unmanned Aircraft (UA), an aircraft, **which is intended to operate with no pilot on board.**

### Application of Drones in Each Sector

**Agriculture**
- Crop health monitoring
- Soil health assessment
- Improved resource utilisation

**Forest and wildlife**
- Wildlife conservation
- Managing human wildlife conflict
- Forest protection

**Urban Development**
- City survey
- Improved urban planning
- Project monitoring
- Project quality assessment

**Healthcare**
- Epidemic control
- Cleanliness & hygiene
- Healthcare delivery

**Traffic Management**
- Road surface condition monitoring
- Improve traffic management
- Traffic feedback

**Homeland Security**
- Real time surveillance
- Security planning
- Drugs/Narcotics detection

**Disaster Management**
- Real time surveillance
- Search and rescue
- Delivery of essential goods

**Mining**
- Mineral scouting
- Managing encroachment
- Contract monitoring

### Need for Drone Regulations

- **Addressing policy gaps** to balance between security concerns and legitimate uses of drones in a variety of civilian sectors.
- **Quality control and standardization** as a sizable percentage of India's drones continue to be imported.
- **Rising use of drones for various sectors** such as agriculture, forest and wildlife, healthcare, mining, disaster management etc.
- **Addressing Privacy Question** as Drones can collect data and images without drawing attention.
- **Terrorist threat management** as there have been several instances of known terrorist organisations using them to carry out their activities.

### Security Concerns with drones

- Drones have been **regularly used to drop weapons and drugs** along the Punjab border. **Conventional radar systems are not meant for detecting** low flying objects.
- **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.
- They **can be controlled from a remote distance** and does not endanger any member of the attacking side.

### Steps taken to regulate and mitigate security risk of drones

- **Draft Drone Rules, 2021** to increase ease of compliance for unmanned aviation industry, and ensure safety and security.
- **Ministry of Civil Aviation had issued National Counter Rogue Drones Guidelines** to deal with rogue drones.
- **Government set guidelines for anti-drone guns** to be deployed by security forces.
- **Detect-and-Destroy technology** for drones developed by DRDO.
- **Drone (Amendment) Rules, 2022** were notified abolishing the requirement of a drone pilot licence.

### Way forward

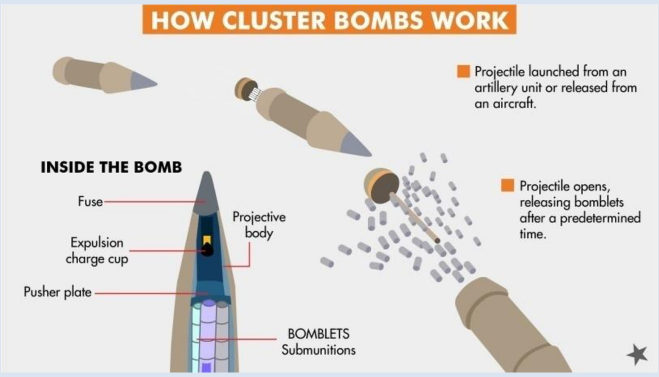
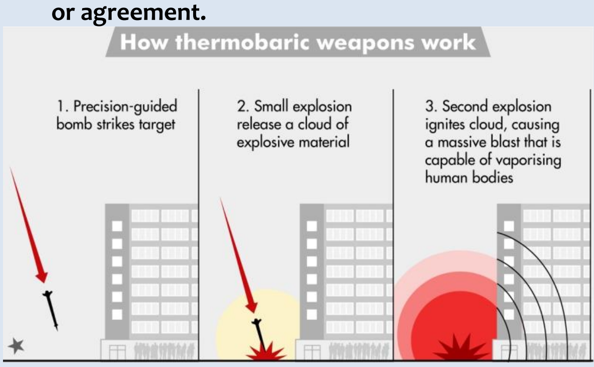
- **An international process to define the limits** of what is acceptable with respect to the possession and use of drones is urgently needed.
- **Government should come up with laws that enable innovation,** but restrict infringements on privacy and misuses of airspace.
- **Rectify classification of Unmanned Aircraft System (UAS)** under the UAS Rules which is weight-based classification rather than performance based.

## 10.3. CLUSTER BOMBS AND THERMOBARIC WEAPON

**Why in News?**

Human rights groups accused Russia of using **cluster bombs and Thermobaric weapons in the ongoing war with Ukraine.**

**About Cluster Bombs and Thermobaric weapon**

| Cluster bombs | Thermobaric weapon (also called aerosol bombs, fuel air explosives, or vacuum bombs) |
|---|---|
| • These are **non-precision weapons** that are designed to injure or **kill human beings indiscriminately over a large area**, and to destroy vehicles and infrastructure.<br>• They **can be dropped from an aircraft or launched in a projectile,** scattering many bomblets as it travels.<br>• Many of these bomblets **end up not exploding**, posing a threat to the civilian population for long after the fighting has ceased.<br>• Countries that have ratified **Convention on Cluster Munitions** are prohibited from using cluster bombs. As of date, **there are 110 state parties to the convention.**<br>○ **Russia, Ukraine, India are not signatories.**<br>• **India has capacity to have cluster munitions delivered by ground**-launched artillery projectiles, rockets, and missiles.<br><br> HOW CLUSTER BOMBS WORK<br>Projectile launched from an artillery unit or released from an aircraft.<br>INSIDE THE BOMB<br>Fuse<br>Projective body<br>Expulsion charge cup<br>Pusher plate<br>BOMBLETS Submunitions<br>Projectile opens, releasing bomblets after a predetermined time. | • They **use oxygen from the air** for a large, high-temperature blast.<br>• **Causes significantly greater devastation** than a conventional bomb of comparable size.<br>• The weapon goes off in **2 separate stages:**<br>○ As they hit their target, a **first explosion splits open the bomb's fuel container**, releasing a cloud of fuel and metal particles that spreads over a large area.<br>○ A **second explosion then occurs,** igniting the aerosol cloud into a giant ball of fire and sending out intense blast waves that can destroy even reinforced buildings or equipment and vaporise human beings.<br>• These are **not prohibited by any international law or agreement.**<br><br> How thermobaric weapons work<br>1. Precision-guided bomb strikes target<br>2. Small explosion release a cloud of explosive material<br>3. Second explosion ignites cloud, causing a massive blast that is capable of vaporising human bodies |

**Related News**

**US warns Russia on usage of Chemical Weapons in Russian - Ukraine War**

| Chemical Weapons | Biological weapons |
|---|---|
| • These are **any kind of munitions that carry toxins or chemical substances** that attack the body's system. It includes<br>○ **Choking agents like phosgene which attack the lungs and respiratory system;**<br>○ **blister agents,** like mustard gas, which burns the skin and blinds people and<br>○ **nerve agents,** which interfere with the brain's messages to the body's muscles<br>• Developing, producing, acquiring, stockpiling, or retaining chemical weapons is prohibited under **Chemical Weapons Convention (CWC).**<br>• CWC was entered into force in 1997 and has **193 states-parties (including India).** | • Biological weapons are thos which **disseminate disease-causing organisms or toxins to harm or kill humans**, animals or plants.<br>○ They **generally consist of two parts** – a weaponized agent and a delivery mechanism.<br>• Development, production, acquisition, transfer, stockpiling and use of biological and toxin weapons is **prohibited under Biological Weapons Convention (BWC).**<br>• It **entered into force in 1975.** It**supplements the 1925 Geneva Protocol,** which had prohibited the use of biological weapons.<br>• It currently has **183 States Parties**(including India). |

## 10.4. HYPERSONIC PLATFORMS

### Why in news?

In August, China reportedly tested a **nuclear-capable hypersonic glide vehicle** that circled the globe before speeding towards its target.

### More about news

- Chinese appear to have combined **a Fractional Orbital Bombardment System**, or FOBS, with a hypersonic weapon. FOBS send missiles through a **partial orbit** around the earth to strike targets **from an unexpected direction.**
- According to the reports, weapon could, in theory, fly **over the South Pole.** That would pose a big challenge for the US military because its **missile defence systems are focused on the northern polar route**.

### About Hypersonic Platforms

- Hypersonic speeds are those that **exceed five times the speed of sound** (Mach 5 or above).
- Hypersonic platforms can be divided into two **main categories:**
  - **Hypersonic Cruise Missiles** (**HCM**): This is typically propelled to high speeds initially using a small rocket, and then, powered to the target by a supersonic combustion ram jet ('scramjet') for hypersonic flight.
  - **Hypersonic Glide Vehicles** (**HGV**): The HGV is a 'boost-glide' weapon. It is first 'boosted' into near-space atop a conventional rocket, and then released at an appropriate altitude and speed.

### How HCM are different from intercontinental ballistic missiles (ICBMs)?

| Intercontinental Ballistic Missiles (ICBMs) | Hypersonic Cruise Missiles (HCMs) |
|---|---|
| • Traditional ballistic missiles and ICBMs arc along a **predictable ballistic path**, like a bullet, and **lack the element of surprise.** | • Hypersonic missile **packs the manoeuvrability** of much slower subsonic cruise missiles and the hypersonic speed **greater than or equal to ICBMs**, making it **harder to track and defend against.**<br>• The **detection-interception time** in case of HCMs and HGVs would be **far less.** Besides, **HGVs do not rise above 100-110 kms** altitude and HCMs fly even lower, at about 20-30 kms altitude. |

### Strategic implications due to growth of Hypersonic Technology

- **Upsets the current military balance of power**.
- **Inadvertent Escalation**: Faced with hypersonic weapons threat and reduced warning-response timings, nuclear-armed states are likely to place their nuclear weapons on a hair-trigger readiness/ 'launch on warning' status.
- **Strategic instability**: Hypersonic weapons, with quick-launch, high-speed, make escalation control very difficult, and generate instability in crisis management at many levels.
- **Nuclear arms race:** Demonstration of Chinese missile prowess has been considered "very close" to a Sputnik moment that suggested the Russians were ahead in the space race leading to nuclear and space race between Russia and U.S.
- **Implications for India:** China's test proves that it is a serious civilian and military threat to India in all areas, including the economy, space, technology, and geopolitics.

**India's progress towards developing hypersonic technology**

- **BrahMos II:** India has collaborated **with Russia** on the development of BrahMos II, a Mach 7 hypersonic cruise missile.
- **Mission Shakti:** To **protect its space assets,** India has already proved its capabilities through the test of indigenously developed **anti-satellite (ASAT) missile technology.**
- **HSTDV:** India is also developing an **indigenous, dual-capable hypersonic cruise missile** as part of its Hypersonic Technology Demonstrator Vehicle programme (HSTDV) and has successfully tested a Mach 6 scramjet.
- **HWT test facility:** is a **pressure vacuum-driven, enclosed free jet facility** that simulates Mach 5 to 12.

### How India should respond to this development?

- **Seize emerging interest in arms control**: to reframe the issue from non-proliferation to non-use of nuclear weapons.

- India can **propose a dialogue on hypersonic weapons** at the Conference on Disarmament and other multilateral fora without forsaking its quest for hypersonic weapons.

- **India should be prepared for arms race:** as power competition among major powers accelerates**.**
- **Space Situational Awareness (SSA):** An independent SSA is crucial for space defence and has the potential to become strategic technology that other countries will require.
- **Investment in technology:** India must move fast and invest heavily in militarised AI technologies to protect its interests at a time when its hostile neighbour is growing stronger at an unprecedented pace.

### Conclusion

Though this test by China is so far done to build capabilities **not against India** but considering relations with China in recent past and unresolved border dispute, India must **develop and test hypersonic capability**, bolstering its **strategic deterrent** against China.

## 10.5. S-400

### Why in News?

Russia started delivery of S-400 Triumf surface-to-air missile system to India.

### About S-400

- S-400 is **among the most advanced air-defence systems** in the world.
  - **Equipped with four different missiles, it can engage** enemy aircraft, ballistic missiles, and Airborne Warning And Control System (AWACS) planes **at 400km, 250km, medium-range 120km and short-range 40km.**
  - It has the capability to engage 80 targets at one time with a **response time of 9-10 seconds.**
- US had offered the anti-ballistic missile defence system Terminal High Altitude Area Defense (THAAD) and Patriot Advanced Capability-3 (PAC-3). Plus, Israel's Iron dome was also one of the options.
  - However, none of the **alternatives offered to India were comparable to the Russian Air Defence System which is considered to be the world's best.**

### Significance of S-400 deal for India

- **Important for national security considerations,** as it faces new threats from China, Pakistan and Afghanistan.
- It will also **offset the air defence capability gaps** due to IAF's dwindling fighter squadron strength.

### Comparison with other major defence systems

| Factor | S-400 by Russia | THAAD by USA | PAC by USA | Iron Dome by Israel |
|---|---|---|---|---|
| **Mobility** | Very High, can be launched within 5 minutes. | Low | Low | Medium |
| **Applicability** | Any topography upto 30 Kms altitude. | Mostly Plain areas | Mostly Plain Areas | Unknown |
| **Range** | 40 to 400Kms with different systems for different ranges providing better security apparatus. | 150 Kms | 100 kms | Single system for 600 Kms range |
| **Special Features** | Capability to track radars and airborne threats upto 600 KMs.<br>Hard to detect and destroy. | Can only counter intercontinental and intermediate range missile systems | Has ability to intercept aerial targets at a range of 180 km only. | Can counter airborne threats but ineffective against lower projectile missiles. |

# APPENDIX: KEY DATA AND FACTS

## DEFENCE

| | |
|---|---|
| Defence Modernisation | ➲ **Initiatives for defence production and indigenization:** Defence Acquisition Procedure (DAP), 2020, iDEX (Innovation for Defence Excellence), SRIJAN Portal, Technology Development Fund (TDF) Scheme etc.<br>➲ **Initiatives for improving military organization:** CDS (proposed by Kargil review committee as well as Shekatkar committee), Integrated Battle Groups, Department of Military Affairs etc.<br>➲ **Other efforts:** Defence Testing Infrastructure Scheme, DRDO's dedicated laboratories for application-oriented research in AI etc. |
| Defence Exports | ➲ **Export increased** from Rs 1,521 crore in 2016-17 **to Rs 13,000 crore in 2021-22.**<br>In 2021-22, **private sector accounted for 70%** of the exports while public sector firms accounted for the rest.<br>➲ Presently, India is exporting **defence equipment to more than 75 countries.**<br>➲ **Major arsenal exported:** Armoured protection vehicles, light-weight torpedo, weapons locating radar, fire control systems, offshore petrol vehicles etc. |
| Self-reliance in Defence Manufacturing | ➲ **Initiatives taken:** DAP, 2020, TDF Scheme, Positive indigenization list, Defence Industrial Corridors, Conducive FDI policy (up to 74% through automatic route) etc.<br>➲ India's **defence expenditure has remained less than 1% of its GDP** in the last five years.<br>➲ India is **funding 6% (on defence R&D)** of Defence Budget compared to USA (12%) and China (20%). |
| Military Logistics Agreements | ➲ Agreements with Australia, Japan, US – **Quad countries – as well as with France, Singapore and South Korea.** |

## DATA PROTECTION

| | |
|---|---|
| Data Protection | ➲ India **does not have any dedicated legal framework** for data protection.<br>➲ **Some acts/judgments cover data protection in general including** IT Act, Right to Privacy Judgement (Justice Puttaswamy case), Consumer Protection Act, Copyrights Act etc.<br>➲ **Personal Data Protection Bill was first brought in 2019** and was referred to JPC.<br>➲ **MeitY has released Draft India Data Accessibility & Use Policy 2022** to harness public sector data for catalysing large scale social transformation. |

## CYBERSECURITY

| | |
|---|---|
| Cyber Crime | ➲ India is **ranked 10th (among 194 countries) in Global Cybersecurity Index 2020.**<br>➲ India has **digitally vulnerable targets with a large pool of over 1.15 billion phones** and more than 700 million internet users.<br>➲ Cost of cyber-attacks is **expected to reach $20 billion n next 10 years.** |
| Regional Cybersecurity | ➲ **Initiatives taken:** Pacific Cyber Security Operational Network (PaCSON), YAKSHA, an EU-ASEAN partnership, Singapore-ASEAN Cybersecurity Centre of Excellence (ASCCE). |

| | |
|---|---|
| Cyber Surveillance | **Implementation of National Automated Facial Recognition System (NAFRS)** to be used by police pan-India.<br>**Communication surveillance in India takes place primarily under two laws:** The Indian Telegraph Act 1885, Information Technology (IT) Act, 2000.<br>**Related SC judgements:** People's Union for Civil Liberties (PUCL) vs Union of India (1997) case, KS Puttaswamy versus Union of India (2017). |
| Critical Infrastructure | **Initiatives for critical infrastructure protection:** National Cyber Security Policy, 2013, National Cyber Security Strategy 2020, CERT-In, National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC) etc |
| Cryptocurrency crime | In 2021, **illicit transactions** using cryptocurrencies were **estimated to be $14 billion,** 79% increase from previous year.<br>Currently, there are **no national guidelines on cryptocurrency related cases.**<br>**India's provisions to control cryptocurrency crime:** Prevention of Money Laundering Act 2002, Indian Penal code, 1860, IT Act 2000. |

## POLICING REFORMS

| | |
|---|---|
| Role of Technology in Law Enforcement | **Technologies used:** Body-worn cameras, automatic tag and license plate readers, Biometrics, Brain fingerprinting, google glass etc.<br>**Best practices in India:** UP (AI enabled app to digitize records of criminals), Punjab (Saanjh-a citizen facing portal), Odisha (MO SAATHI to help women), Maharashta (AMBIS database of criminals) etc. |
| Modernisation of Police Force | **Nearly 20% of the sanctioned strength is vacant** at various levels.<br>Despite rising cyber-crimes, **several states like Punjab, Rajasthan, Goa, Assam do not have a single cyber-crime cell.**<br>Modernisation of Police Forces (MPF), **a centrally sponsored scheme by MHA.**<br>**Some experts body for police reforms:** Padmanabhaiah Committee (2000), Malimath Committee (2002-03), SC directives in Prakash Singh Case (2006), Second ARC (2007), Police Act Drafting committee II (2015).<br>**Government Initiatives:** SMART Policing, Crime and Criminal Tracking Network System (CCTNS), Model Police Act, 2006 etc. |

## EXTREMISM AND TERRORISM

| | |
|---|---|
| Naxalism | **LWE violence has decreased** from 2258 in 2009 to 509 in 2021.<br>**Only 46 districts** reported LWE related violence in 2021 as **compared to 96 districts in 2010.**<br>**Deaths (civilians and security forces) have reduced by 85%** in 2021 from 2010.<br>**Initiatives taken for LWE states:** National Policy and Action Plan (2015), Various Sub –Schemes under Scheme Modernization of Police Forces, SAMADHAN strategy.<br>**Skill Development:** ROSHINI, ITIs and Skill Development Centres, livelihood college etc.<br>**Institutional measures:** Black Panther combat force for Chattisgarh, Bastariya Batallion etc. |
| Bio-Terrorism | **Existing measures in India:** Epidemic Diseases Act of 1897, NDMA proposed a model instrument for government and private sector, Integrated Disease Surveillance Project.<br>**Measures at International Level:** Biological Weapons Convention, INTERPOL Bioterrorism Prevention Unit, Cartagena Protocol on Biosafety. |
| UAPA (Unlawful Activities [Prevention] Act | Only **3.1% of cases registered UAPA cases between 2018 and 2020 resulted in conviction.** |

| | |
|---|---|
| Overground Workers | **Steps taken to deal with OGW:** Operation All Out, Operation Sadbhavna, Mission Pehal, USTTAD, Nai Manzil scheme, Opportunities under HIMAYAT |
| Drug Trafficking | As per UNODC 2022 report, **India is one of the world's single-largest opiate markets in terms of users.**<br>**India has become a transit hub as well as a destination** for heroin and hashish produced in Golden Triangle and Golden Crescent.<br>Within India, the **worst affected regions are North East India** (especially Manipur) and North West India (especially Punjab). |

# INSURGENCY IN NORTHEAST

| | |
|---|---|
| Initiatives taken to restore peace | **Fencing of borders** with regional cooperation, **priority to northeast routes under UDAN 4.0,** development as **economic hub under Act East Policy** (National Bamboo Mission, Agri export Zones etc.).<br>**3rd Bodo Peace Accord** (2020) was signed for peace in Bodo-dominated areas in Assam.<br>Government **entered into ceasefire Agreement** with National Socialist Council of Nagaland (K) Niki Group. |

# EMERGING DIMENSIONS OF SECURITY

| | |
|---|---|
| Space Weaponisation | **India in the race of space power:** Indian National Committee for Space Research (INCOSPAR) formed in 1962, ISRO in 1969, Defence Space Agency (DSA) in 2019, Anti-satellite (ASAT) missile test (Mission Shakti).<br>**Global Framework to prevent Weaponization of Space:** Outer Space Treaty, Prevention of an Outer Space Arms Race. |
| Emerging Technologies and Threats to Nation | MEA created a **New, Emerging and Strategic Technologies (NEST) division,** National Supercomputing Mission, National Mission on Quantum Technologies & Applications etc. |

# MISCELLANEOUS

| | |
|---|---|
| Internet Shutdowns | There have been **around 550 internet shutdowns in India so far** since 2012 and Internet shutdowns in **2020 cost India $2.8 bn.**<br>**Rules/legal provisions for Internet shutdown:** Temporary Suspension of Telecom Services (Public Emergency & Public Safety) Rules, 2017, Supreme Court Judgement in 2020. |
| Hypersonic Platforms | **India's progress towards developing hypersonic technology:** BrahMos II, Mission Shakti, Hypersonic Technology Demonstrator Vehicle programme (HSTDV) etc. |

# WEEKLY FOCUS

## Security

| TOPIC | 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. | |

# 8 IN TOP 10 SELECTIONS IN CSE 2021

*from various programs of VisionIAS*

2 AIR

ANKITA AGARWAL

## CIVIL SERVICES EXAMINATION 2020

1 AIR

SHUBHAM KUMAR

3 AIR

GAMINI SINGLA

4 AIR

AISHWARYA VERMA

5 AIR

UTKARSH DWIVEDI

6 AIR

YAKSH CHAUDHARY

7 AIR

SAMYAK S JAIN

8 AIR

ISHITA RATHI

9 AIR

PREETAM KUMAR

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