VISIONIAS
INSPIRING INNOVATION

# MAINS 365

# SECURITY

Classroom Study Material 2019

( September 2018 to June 2019 )

www.visionias.in
+91 8468022022

DELHI | JAIPUR | PUNE | HYDERABAD | AHMEDABAD | LUCKNOW

# SECURITY

## Table of Contents

# 1. CYBER SECURITY

- Cyber security means **securing the cyberspace** from attack, damage, misuse and economic espionage. Cyberspace is a **global domain within the information environment** consisting of interdependent IT infrastructure such as Internet, Telecom networks, computer systems etc.
- The **2019 Global Risk Report** (World Econonmic Forum) highlights India's history of malicious cyber-attacks and lax cybersecurity protocols which led to massive breaches of personal information in 2018.
  - It also specifically mentions the government ID database, Aadhaar, which has reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens.
- In 3rd Global Cybersecurity Index released by the International Telecommunication Union, India slipped to 47th rank in 2018 from 23rd in 2017.

**Need for cybersecurity**

- **Government's digital push**: Various programs of government such as Aadhaar, MyGov, Government e-Market, DigiLocker, Bharat Net etc. are prompting a larger number of citizens, companies and government agencies to transact online.
- **Start-ups digital push**: India is the third largest hub for technology-driven startups in the world and its ICT sector is estimated to reach $225 billion landmark by 2020.
- **Increasing vulnerability**: India the fifth most vulnerable country in the world in terms of cybersecurity breaches. India saw at least **one cybercrime every 10 minutes** during the first half of 2017 including more sophisticated cyber threats such as the **WannaCry and Petya** ransomware.
  - India accounted for 5.09 per cent of all cyberattacks such as malware, spam and phishing attacks detected globally in 2017.
- **Prevent economic loss**: The estimated cost of cyber-attacks in India stands at four billion dollars which is expected to reach $20 billion in the next 10 years.
- **Increasing internet users:** India ranks 3rd in terms of number of internet users after USA and China. By 2020, India is expected to have 730 million internet users with 75% of new users from rural areas.
- **Increasing online transactions:** For e.g.: by 2020, 50% of travel transactions will be online and 70% of e-commerce transactions will be via mobile.

**Types of cybercrime**

- **Cyber Warfare:** states attacking the information systems of other countries for espionage and for disrupting their critical infrastructure.
- **Phishing:** It is a kind of fraudulent attempt that is made through email, to capture personal and financial information.
- **Cyber Stalking:** repeated use of electronic communications to harass or frighten someone
- **Identity theft:** It is a type of fraud in which a person pretends to be someone else and does crime with the name of someone else
- **Denial of service (DoS):** It attacks refers an attempt to make computer, server or network resources unavailable to its authorized users usually by using temporarily interruption or suspension of services.

**Challenges in ensuring cyber security**

- **Widespread digital illiteracy:** which makes Indian citizens highly susceptible to cyber fraud, cyber theft, etc.
- **Using Substandard devices**: In India, majority of devices used to access internet have inadequate security infrastructure making them susceptible to malwares such as recently detected **'Saposhi'.**
  - Rampant use of unlicensed software and underpaid licenses also make them vulnerable
- **Lack of adoption of new technology:** For e.g.: Banking infrastructure is not robust to cop-up with rising digital crime as 75% of total Credit and Debit card are based on magnetic strip which are easy to be cloned.
- **Lack of uniform standards**: There are variety of devices used with non-uniform standards which makes it difficult to provide for a **uniform security protocol.**
- **Import dependence:** for majority of electronic devices from cellphones to equipments used in power sector, defence and other critical infrastructure put India into a vulnerable situation.
- **Lack of adequate infrastructure and trained staff:** There are currently around 30,000 cyber security vacancies in India but demand far outstrips supply of people with required skills.
- **Anonymity:** Even advanced precision threats carried out by hackers is difficult to attribute to specific actors, state or non- state.

- **Lack of coordination among various agencies working for cyber security.** Further, Private sector, despite being a major stakeholder in the cyberspace, has not been involved proactively for the security of the same.
- **Other challenges:** include absence of geographical barriers, majority of servers located outside India, rapidly evolving technology in cyberspace and difficulty in establishing a foolproof cybersecurity architecture because of number of vulnerable points in the overall ecosystem.

**Various steps taken**

- **Institutional Measures**
  - **National Critical Information Infrastructure Protection Centre (NCIIPC)** to battle cyber security threats in strategic areas such as air control, nuclear and space. It will function under the National Technical Research Organisation, a technical intelligence gathering agency controlled directly by the National Security Adviser in PMO.
  - **National cyber coordination centre (NCCC)** to scan internet traffic coming into the country and provide real time situational awareness and alert various security agencies.
  - A **new Cyber and Information Security** (CIS) **Division** has been created to tackle internet crimes such as cyber threats, child pornography and online stalking.
    - ✓ Under this, **Indian cyber- crime coordination centre** (I4C) and **Cyber Warrior Police force** has also been established.
  - Ministry of Defence formed **Defence Cyber Agency** in the realm of military cyber security.
  - **Indian Computer Emergency Response Team (CERT-in)** to enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration.
    - ✓ **CERT-fin** has also been launched exclusively for financial sector.
    - ✓ CERT-in is also operating **Cyber Swachhta Kendra**, a Botnet Cleaning and Malware Analysis Centre.
  - Government inaugurated the new body **National Information Centre-Computer Emergency Response Team** (NIC-CERT) to prevent and predict cyber-attacks on government utilities.
  - **Cyber Surakshit Bharat Initiative** to strengthen Cybersecurity ecosystem in India. It is first public-private partnership of its kind and will leverage the expertise of the IT industry in cybersecurity.

**Critical information infrastructure**

- Critical information infrastructure is communications or information service whose availability, reliability and resilience are **essential to the functioning of a modern economy, security and other essential social values.**
- Critical information sectors in India include **Power, ICT/Communication, Finance/Banking, Transport and e-governance.**
- The complex interactions among various industrial functions of critical infrastructure and the exchange of information leads to **"interdependencies".** A minor disruption at one point could have a rippling effect across multiple infrastructures.
- Critical infrastructure protection is basically a **two-step approach.**
  - To identify the plausible threats
  - To identify and reduce the vulnerabilities of individual systems to any sort of damage or attack and reduce their recovery time.

**International Measures**

- **Cyber-diplomacy:** India has entered into cyber security collaborations with countries such as the USA, European Union and Malaysia. For eg- U.S.-India Cyber Relationship Framework
- **Global Conference on Cyber Space (GCCS):** A prestigious global event where international leaders, policymakers, industry experts, think tanks, cyber wizards etc. gather to deliberate on issues and challenges for optimally using cyberspace. Fifth GCCS was held in India.
- **Global Centre for Cybersecurity:** It was launched by the World Economic Forum (WEF) to serve as laboratory and early-warning think tank for future cybersecurity scenarios and help build a secure global cyberspace.

**Other norm building initiatives**

- **Microsoft** launched its **"Digital Peace" campaign** along with a **Cybersecurity Tech Accord** aimed at getting internet & technology industry to better protect their customers' privacy & security against cyber attacks.
- **Siemens** unveiled a **Charter of Trust** that seeks to develop adherence to security principles & processes, with the aim of developing a "global standard" for cyber-security.
- In 2015, a **Group of Governmental Experts (GGE)** at the UN charted **4 peace time norms** in the cyberspace:
  - No interference with each other's critical infrastructure by states
  - Assistance to other nations in investigating cyber attacks
  - Not targeting each other's computer emergency response teams
  - Responsibility of states for actions originating from their territory.

- The Ministry of Home Affairs is implementing the **'Cyber-Crime Prevention against Women & Children'** Scheme.

- **Legislative Measures**
  - **Information Technology Act, 2000 (amended in 2008)** to provide a legal framework for transactions carried out by means of electronic data interchange, for data access for cybersecurity etc. Some of the prominent provisions are:
    - ✓ **Section 43:** Data protection
    - ✓ **Section 66:** Hacking
    - ✓ **Section 69:** Cyberterrorism
  - **National Cyber Security Policy 2013**: The Policy proposed to:
    - ✓ Set up different bodies to tackle various levels of threats, along with a national nodal agency to coordinate all cybersecurity matters.
    - ✓ Create a National Critical Information Infrastructure Protection Centre (NCIIPC)
    - ✓ Create a workforce of around 500,000 trained in cyber security.
    - ✓ Provide fiscal benefits to businesses to adopt best security practices.
    - ✓ Set up testing labs to regularly check safety of equipment being used in the country.
    - ✓ Create a cyber ecosystem in the country, developing effective public-private partnerships and collaborative engagements through technical and operational cooperation
    - ✓ Build indigenous security technologies through research.

**Way forward**

- **Ensure coordination:** National Cybersecurity Coordinator (NCC) may be strengthened to bring about much-needed synergy among various institutions and work out a coordinated approach to cyber security, including cyber deterrence.
- **Cyber deterrence:** It is of two kinds – defensive and offensive. India needs to make a proper assessment of an offensive cyber doctrine adopted by many countries where they are acquiring offensive capabilities by building bits of software called 'cyberweapons' to do enormous damage to the adversary's networks.
- **Better regulation and adoption of norms:** Presently, there are no acceptable norms of behaviour in cyberspace. Thus, state as well as companies are developing their own capabilities leading to unchecked proliferation of offensive cyber tools and practices having potential to destabilise the entire cyberspace.
- **Establishing cyber insurance framework:** Currently the average cost of a cyber insurance in India is around $7.5 million which in comparison to developed countries is about 20-25% lesser.

**Related Information**

**About Budapest convention on cybercrime**

- This convention of the council of Europe is **the only binding international instrument** on this issue that addresses Internet and computer crime by harmonizing national laws, improving legal authorities for investigative techniques, and increasing cooperation among nations.
- It deals with issues such as infringements of copyright, computer-related fraud, child pornography and violations of network security.
- It aims to pursue a common criminal policy, especially by adopting appropriate legislation and fostering international police as well as judicial co-operation.
- It is supplemented by a "Protocol on Xenophobia and Racism" committed through computer systems
- The Convention has 56 members, including the US and the UK. **India is not yet a member.**

**Why India should join?**

- India would **benefit from a proven framework** under which nations commit to cooperate with each other to the widest extent possible with respect to cybercrime, and any crime involving electronic evidence.
- The convention **can be the foundation for a global law on cybersecurity** and may **help in guiding national legislation** or policy against cybercrimes.
- India would become a priority country for capacity-building and would be able to contribute to shaping future solutions if it were a party.

**Arguments against joining**

- Developing countries including India have not signed it stating that the developed countries drafted it without consulting them.
- Its specific provisions fail to protect rights of individuals and states.
- The mutual legal assistance by convention is too complex & lengthy, rendering it inefficient in practice.
- Intelligence Bureau (IB) has raised concern that it infringes upon state sovereignty. For eg- an Article of the convention allows local police to access servers located in another country's jurisdiction, even without seeking sanction.

- **Promote investment in cybersecurity by businesses:** Investment in IT security has to be increased with adoption of a cybersecurity plan, purchase of cyber-insurance as well as appointment of a data security officer.
- **Amendment of IT Act 2008:** The regulations need to keep pace with the changing cyber scenario to ensure penalties serves as deterrence for crimes. For ex: In the Indian IT act, financial fraud is a still a bailable offence.
- **Skill development:** By 2025, the cybersecurity space is expected to generate around a million jobs in India. To avoid ceding jobs to expatriates, India must establish ecosystem to develop necessary skills. The idea of a National Cyber Registry "as a repository of IT professionals" may also be implemented.
- **Updation of cyber security policy:** India needs an updated policy on cybersecurity as **National Cyber Security Policy 2013** outlined the broad principles regarding how to approach cybersecurity while lacking outline to operationalise it.
- **Security audit:** Security Audit adhering to international standards may be made applicable for all govt. websites, applications before hosting and publishing.
- **Establishing cybersecurity framework at state level:** For eg- establishment of state CERT to work in conjunction with CERT-in
- **Enhanced international cooperation:** There must be enhanced cooperation among nations and reaffirmed a global call to action for all United Nations member nations to not attack the core of the Internet even when in a state of war. Recently, Ministry of home affairs called for signing of the **Budapest Convention on cybercrime** owing to the surge in cyber-crime.

**Conclusion**

Cybersecurity is an increasingly important part of our life today, and the degree of interconnectivity of networks implies that anything and everything can be exposed, and everything from national critical infrastructure to our basic human rights can be compromised. Governments are therefore urged to consider policies that support continued growth in technology sophistication, access and security, and as a crucial first step, to adopt a national cybersecurity strategy.

## 1.1. PARIS CALL

**Why in news?**

At UNESCO Internet Governance Forum (IGF) meeting convened in Paris, **"The Paris Call for Trust and Security in Cyberspace"** was commenced, aimed at developing common principles for securing cyberspace.

**Principles articulated in the Paris Call**

The goals mentioned in the Paris Call and the principles adopted represent a consensus of priorities between states, corporations and civil society.

- **Inclusive regulatory process:**
  - Gather existing sector-specific initiatives (Tech Accord, UN's Group of Government Experts, For The Web) in a single document and widen their scope, to set out a framework for further negotiations.
  - Recognize the responsibilities of private sector actors in improving trust, security and stability in cyberspace.
  - Adopt a **strong multi-stakeholder approach to improve collaboration** among government, private sector and civil society to tackle the threat of cyber criminality. Budapest Convention on Cybercrime is a key tool in this regard.
- **International Law:**
  - Encourage better coordinated regulation of cyberspace and use of information & communication technologies (ICT) in the spirit of principles of U.N. Charter & international humanitarian law, notably the maintenance of international peace and security.
- **State sovereignty**
  - Promote the exclusive role of sovereign states in hostile acts in cyberspace. It condemns corporate hack-back and other offensive operations from non-state actors.
  - It also appeals for measures preventing interference with elections.

- **Protection of citizens**
  - Protect individuals and critical infrastructure from harm & safeguard the "public core of the Internet" from hostile actors
  - Engage industries and civil society in promoting everyday good practices ("cyber hygiene") and the implementation of "security by design" in products and services. Cyber hygiene refers to data protection and safety at an individual level.

**Who joined?**

- More than 190 signatures were obtained on the Paris Call, including 130 from private sector and more than 50 member nations. Prominent countries like **India, US, China, Russia didn't sign the agreement.**
- **Several major American technologies** like Facebook, Microsoft, Google, IBM, HP etc. have **endorsed the agreement**.

**Significance of Paris Call**

- Paris call gives a fresh momentum to the issue of **creating globally acceptable cyber security norms** by mounting support from multiple stakeholders.
- It could also be seen as a positive step towards finding a **middle path between Western democracies and authoritarian regimes** so as to build some form of consensus on issues pertaining to cyberspace.
- However, there are **some issues** that are yet to be ironed out. This includes:
  - Putting in place legally binding compliance mechanism
  - Dealing with espionage and state-lead offensive operations, particularly through non-state proxies doing state's bidding.
- While the US, China and Russia are unlikely to join, the call will depend on support from states like India in order to gain traction within international institutions, primarily the United Nations.

**Models of Internet Governance**

- **Multi-stakeholder Model (supported by western nations like US)**
  - Decentralized governance institutions where non-state actors like corporates, NGOs & civil society have a say in making globally acceptable norms regulating cyberspace.
  - Gives recognition to technical expertise of corporates.
- **Multilateral Model (supported by Russia and China)**
  - Governance model based on agreements between multiple governments with limited involvement of non-state actors.
  - Holds sovereignty of nation state in managing cyberspace and provides the scope for the exercise of inherent right of self-defense and the law of state responsibility, including countermeasures in the cyberspace.

**India's Stand**

- India stance has gradually shifted to multi-stakeholderism from long supported multilateralism.
- However, India envisages a **pivotal role for governments as the custodian of cyberspace** in the areas of international security and public policy. This is evident from its stand on data localization (wants storing of data within the country) and server management.
- India also supports greater cooperation from corporates in terms of data sharing to tackle cyber crimes.
- Currently, the engagement – at both government & private level - with the global policymaking apparatus has been low, including participation at Internet Corporation for Assigned Names and Numbers (ICANN) summits.
- India should begin with initiating domestic multi-stakeholder engagement (India Internet Governance Forum) to engage civil society and technical experts adequately in pursuit of multi-stakeholderism.

# 2. SECURITY IN BORDER AREAS

## 2.1. BORDER MANAGEMENT

- India has a **land border of over 15,000 kms**, which it shares with seven countries (Pakistan, China, Bangladesh, Nepal, Myanmar, Bhutan, and Afghanistan). Further, it has a **coastline of over 7,500** kms.
- The **Ministry of Home Affairs is responsible for management of international lands and coastal borders**, strengthening of border guarding and creation of infrastructure such as roads, fencing, and lighting of borders.

**Need for effective border management**

The proper management of borders is vitally important for national security. Different portions of our extensive borders have a variety of problems which have to be appropriately addressed. Some of the common problems affecting the management of border security include:

- **Lack of proper demarcation** of our land and maritime borders.
- **Complex and different terrain** on all borders makes it difficult to attain specialization in border management.
- **Lack of coordination** among multiple agencies associated with border security.
- **Lack of infrastructure** with border forces including shortage both in terms of manpower and infrastructure.
- **Inadequate attention to the concerns of local people** in border areas which is exploited by hostile elements to create a feeling of ill will against the security forces & Government.
- **Inadequate attention to security forces** such as no mobile connectivity leading to isolation, inadequate medical facilities, disparity in wages and allowances in comparison with the army.

| Border | Challenges along the border | Recent initiatives by government |
|---|---|---|
| Indo-China | • **Border dispute** at Aksai Chin, Arunachal Pradesh, Doklam etc. with sporadic aggression.<br>• **Large scale smuggling** of Chinese **electronic and other consumer goods** take place through these border points even after designated areas for border trade.<br>• **Inadequate infrastructure** due to difficult terrain. However, China has undertaken a large-scale effort to upgrade air, roads and rail infrastructure, as well as surveillance capabilities near to the border.<br>• **Multiple forces along Indian border** (for e.g.-ITBP, Assam rifles, Special frontier force) as opposed to single PLA commander on Chinese side.<br>• **Water-sharing issue** as China is building dams on its side reducing water flows on our side. | • **Creating infrastructure: India is also constructing some critical bridges to cut down time for troop movement such as Dhola- Sadiya bridge.**<br>• India has **joined hands with Japan to aggressively develop infrastructure projects in North east to contain China.**<br>• **Army infrastructure projects within 100Km of LAC have been** exempted from forest clearance.<br>• **To expedite border road construction, Ministry of Defence has decided to delegate administrative and financial powers to the Border Roads Organisation (BRO).** |
| Indo-Pak | • **Border dispute** at Sir Creek and Kashmir.<br>• **River water sharing issue** at Indus river.<br>• **Infiltration and Cross-border terrorism** targeted to destabilise India. Recently BSF detected a fifth (since 2012) cross-border tunnel in the forest area of Jammu.<br>• **Diverse terrain** including desert, marshes, snow capped mountain and plains makes border guarding difficult.<br>• **Time & cost overruns** in infrastructure projects due to unforeseen | • **Following Pathankot terrorist attack, MHA sanctioned the implementation of** Comprehensive Integrated Border Management System **(CIBMS) to establish an integrated security system at borders providing all-round security even in adverse climatic conditions.**<br>• **The centre has decided to deploy Indian special forces unit** National Security Guard (NSG) commandos in J&K **to fortify** counter terror **operations by training J&K** |

| | | |
|---|---|---|
| | **circumstances& natural calamities.**<br>• **Other issues include drug smuggling, fake currency, arms trafficking.** | **police and other paramilitary forces in room intervention, anti-terror skills, overseeing anti-hijack operations etc.** |
| Indo-Nepal | • Increasing Extremism and anti-India activities due to increasing activities of ISI such as pushing in men and explosives through the border.<br>• Fear of spread of **Maoist insurgency** due to links of Nepal's Maoists in India.<br>• **Easy escape & illegal activities** - Insurgents, terrorists, many hard-core criminals pursued by Indian and Nepalese security forces escape across the open border.<br>✓ These anti-national elements indulge in illegal activities, such as smuggling of essential items and fake Indian currency, gun-running, and drugs and human trafficking.<br>• **Other issues:** Disputed border at times lead to land grabbing on each side. | • **Establishment of a new intelligence section in SSB at Indo-Nepal and Indo-Bhutan border to ensure better operational efficiency.**<br>• **Establishment of Border District Coordination Committee at the level of district officials of the two countries to discuss issues of mutual concern.**<br>• **The Government of India has approved construction of 1377 km of roads along Nepal border.**<br>• **Development aid to Nepal to prevent human trafficking owing to lack of employment opportunities there.** |
| Indo-Bhutan | • **Insurgency-** Many groups such as Bodo, ULFA etc. sneak into Bhutan for sanctuary despite their army driving them out.<br>• Smuggling of goods such as Bhutanese cannabis, liquor and forest products.<br>• Free movement of people and vehicle leading to issues such as during the Gorkhaland movement in West Bengal. | • **Bilateral cooperation - A Secretary level bilateral mechanism in the shape of an India- Bhutan Group on Border Management and Security.**<br>• **Cooperation with their army to prevent sanctuary to insurgents in their soil.**<br>• Establishing new border posts **in Sikkim along the Bhutan frontier near Doklam.**<br>• **The Union environment ministry has given a "general approval" for the diversion of forest land for major border infrastructure projects along the eastern border with Bhutan, Myanmar and Nepal.** |
| Indo-Myanmar | • **Free movement Regime:** Insurgents are misusing FMR to cross-over to Myanmar and receive training and acquire arms.<br>• Drug trafficking due to proximity to golden triangle.<br>• Weak borders as there is practically no physical barrier along the border either in the form of fences or border outposts and roads to ensure strict vigil.<br>• Poor Infrastructural facilities at Moreh and Zokhawatar – the two designated points for normal trade and border trade. | • **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. ICP is able to interdict such elements while facilitating legitimate trade and commerce.** |
| Indo-Bangladesh | • **Water disputes such as sharing of Teesta river, construction of Dam by India on Barak river.**<br>• **Illegal migration: Since the 1971 war of independence that created the state of Bangladesh, millions of Bangladeshi immigrants (the vast majority of them illegal) have poured into India.**<br>• **Inadequate border fencing due to issues such as riverine areas, protests by residing population, pending land acquisition etc.**<br>• **Trafficking of goods like jamdani sarees, rice salt etc. as well as cattle smuggling.** | • **Government has announced the establishment of Border Protection Grid (BPG) with Indo- Bangladesh Border States.**<br>• **A crime-free stretch has been established between the BSF border posts at Gunarmath and Kalyani and the BGB (Border Guards Bangladesh) border posts at Putkhali and Daulatpur.**<br>• **Installation of Border surveillance devices such as closed-circuit cameras, search-lights, thermal imaging devices and drones to keep a tight vigil.**<br>• **The BSF and BGB have also been raising awareness among the locals regarding crime prevention in the border area.** |

**Other Steps that need to be taken further**

- **Dispute resolution**- Government should resolve pending border disputes with the neighbouring countries, as they later become matters of national-security threat.
- **No diversion of security forces**- The border-guarding force should not be distracted from its principal task and deployed for other internal security duties. For eg-ITBP, a force specifically trained for India-China border should not be used in the naxalite-infested areas.
- **Involvement of army** – It is felt that the responsibility for unsettled and disputed borders, such as the LoC in J&K and the LAC on the Indo-Tibetan border, should be that of the Indian Army while the BSF should be responsible for all settled borders.
- **Follow one-force-one-border principle** to effectively manage borders as divided responsibilities never result in effective control.
- **Developing Infrastructure**-accelerated development of infrastructure along the border, especially to wean the border population from illegal activities.
- **Use of advanced technology** - The advances in surveillance technology, particularly satellite and aerial imagery, can help to maintain a constant vigil along the LAC and make it possible to reduce physical deployment.
- **Up-gradation of intelligence network** and co-ordination with sister agencies, conduct of special operations along the border.
- Raising the issues of infiltration from across the border during various meeting with counterpart countries.

## 2.1.1. ROLE OF TECHNOLOGY IN BORDER MANAGEMENT

**Why in news?**

Recently, Union Home Minister inaugurated the **smart border fencing project** and the **project BOLD-QIT (Border Electronically Dominated QRT Interception Technique)** under the comprehensive integrated border management system (CIBMS) programme.

**Role of technology in border management**

- **Upgrading existing system:** Technology can be **integrated with the existing systems** to facilitate better detection and interception by the man behind the machine.
- **Checking infiltration:** It can be help to detect infiltration via land, underwater, air and tunnels by deploying close-circuit television cameras, thermal imagers and night vision devices etc.
- **Facilitate Cross Border Trade:** For example: Blockchain technology can help quickly and securely process transactions, it also makes much easier to identify and trace illegitimate trade.

**Comprehensive Integrated Border Management System (CIBMS)**

- It is a robust and integrated system that is capable of addressing the gaps in the present system of border security by seamlessly integrating human resources, weapons, and high-tech surveillance equipment.
- It has three main components:
  - **New high-tech surveillance devices** such as sensors, detectors, cameras, etc. as well as existing equipment for round-the-clock surveillance of the international border.
  - **An efficient and dedicated communication network** including fiber optic cables and satellite communication for transmitting data gathered;
  - **A command and control centre** to which the data will be transmitted providing a composite picture of the international border.
- **Smart fencing at the borders** under CIBMS is a technological solution devised to address the security issues in the Border States.
- **BOLD-QIT** under CIBMS is the project to install technical systems under the CIBMS, which enables BSF to equip Indo-Bangla borders with different kind of sensors in unfenced riverine area of Brahmaputra and its tributaries.

**Issues which India might face in implementation**

- The system might **suffer numerous technical glitches** such as a large number of false alarms, line of sight constraints, unreliable information transmission, and equipment malfunction.
- At present, many of the high-tech surveillance devices deployed by the BSF are **not optimally utilized** because the required technical expertise is not uniformly available among the force's personnel.
- The **exorbitant cost of the electronic devices** and the lack of easy availability of spare parts act as a deterrent against their use.
- **Erratic power supply and adverse climatic and terrain conditions** in the border areas could potentially undermine the functioning of the sophisticated system.

- **Facilitate Communication:** It can be used for better coordination among various stakeholders by providing timely information.
  - **Deployment of Central Armed Police Forces (CAPFs)** in remote areas will be also coordinated through satellite communications.
  - **Deployment of dedicated communication satellites:**
    - ✓ **GSAT 7** is the first dedicated military communication satellite built by ISRO that will provide services to the Indian defence forces with the main user being the Indian Navy.
    - ✓ **GSAT-7A** is meant primarily for the Indian Air Force with Indian Army using 30% of capacity.
    - ✓ India uses the RISAT and Cartosat satellites to capture still images as well as high-resolution video of the nation's disputed borders.
- **Improved Intelligence inputs and Surveillance:** through Remote sensing satellites, radar satellites and satellites with synthetic aperture radar (SAR) sensors which are capable of providing day and night all-terrain and all-weather inputs.
- **Facilitate Navigation: Indian Regional Navigation Satellite System (IRNSS)-based GPS** will provide navigation facilities for operational parties in high altitude, remote and difficult borders, and Maoist-affected areas.

## 2.1.2. MARITIME/COASTAL SECURITY

**Why in news?**

Recently, India commemorated 10 years of Mumbai attacks.

**More on news**

- One of the deadliest terror attacks to be staged on Indian soil, it exposed several lacunae in Indian security infrastructure, making it a **'watershed' moment in India's internal security paradigm**.
- It exposed **India's maritime security vulnerabilities** including absence of deep sea surveillance and malfunctioning coastal policing.
- It also brought to notice the issues in **intelligence coordination, absence of defined crisis reportage protocols and slow response to the attack.**

**Coastal Security vulnerability in India**

- India's coasts are characterised by a **diverse range of topography** such as creeks, small bays, back waters, rivulets, lagoons, swamps, beaches, small islands (inhabited as well as uninhabited) etc.
- India's long coast line presents a **variety of security concerns** that include: smuggling of arms and explosives, infiltration, piracy etc.
- **Absence of physical barriers on the coast** and presence of vital industrial and defence installations on it enhances the vulnerability of the coasts to illegal cross border activities.
- Various coastal borders of India are close to politically volatile, economically depressed and unfriendly countries such as Sri Lanka, Bangladesh, Pakistan and Gulf countries making it even more vulnerable.

**Other Steps taken by government for coastal security**

- **Indian Maritime Security Strategy (IMSS) 2015 of Indian Navy**: It envisages greater coordination between different maritime agencies; securing Indian Ocean sea lines of communication (SLOCs); Maritime Security Operations for contemporary assessments of maritime terrorism, piracy etc.; multilateral maritime engagement, local capacity building, technical cooperation etc.
- **Coastal Security Scheme (CSS)** to strengthen security infrastructure of Marine Police Force in coastal states/UTs.
- **Central Marine Police Force (CMPF):** to protect sea, coasts, ports and vital institutions and investigate crimes committed in the coastal water.
- **Involving fishermen in surveillance & intelligence gathering**: Fishermen groups, referred to as the 'ears and eyes' of coastal security, are created comprising of trained volunteers who monitor the seas and coastal waters.
- **Enhance Maritime Domain Awareness:** through National Command Control Communication and Intelligence Network (NC3I), an over-arching coastal security network which collates and disseminates data about all ships, dhows, fishing boats and all other vessels operating near our coast.
- **Capacity building**-The Navy and Coast Guard have also provided periodic maritime training to marine police in all coastal states.
- **Indian Ocean Naval Symposium** to provide an open and inclusive forum for discussion of regionally relevant maritime issues.

**Improvements in coastal security mechanism since 26/11**

- The institutional setup for the coastal security includes the **National Committee for Strengthening Maritime and Coastal Security at the apex level**. It coordinates all matters related to Maritime and Coastal Security and periodically reviews coastal security against threats from the sea with all stakeholders.
- **3-layered protection** of Indian coastal areas has been strengthened and responsibilities have been clearly delineated.
  - **Indian Navy:** Beyond 200 Nautical Miles (NM)
  - **Indian Coast Guard:** 12 to 200 NM
  - **Marine Police:** Up to 12NM from shore
- **Coastal Surveillance Network**, comprising of static sensors along coasts, automatic identification systems (AIS), long range tracking, day-night cameras and communication devices has been put in place. **Vessel Traffic Management System (VTMS)** radars are installed on all major & minor ports to facilitate surveillance.
- Commissioning of **Information Management & Analysis Centre (IMAC)** in Gurugram for easy collection and dissemination of shipping data for increased awareness.
  - The Navy established the **Information Fusion Centre for the Indian Ocean Region (IFC-IOR)** at IMAC for 24/7 regional information sharing on commercial shipping.
- **Activities in maritime zones are now more regulated**: (i) Multi-purpose ID issued to all fishermen, sea-ferrying services and coastal villages (ii) Uniform licensing of fishing boats (iii) GPS and transponders for tracking.
- **Central Industrial Security Force (CISF)** now guards ports. Moreover, **Sagar Prahari Bal** was constituted as a special force from navy for protection of naval bases.
- **Operation Sagar Kavach** was put in operation post 26/11 to improve coordination between security agencies including Indian Navy, Coast Guard and the local police.

**Issues remaining in coastal security**

- **Shortage of manpower:** The marine police stations are not functioning effectively due to shortage of manpower and lack of interceptor boats.
- **Inadequate training for marine police:** Though marine police is tasked with overall coastal security but they are not trained for counterterrorism.
- **Lack of a cooperative mechanism**: Many agencies like Navy, Coast Guard, Marine Police and other authorities are tasked with coastal security. Hence the information sharing and coordination is a major problem.
- **Inadequate mechanisms at state level:** There is below par state-level monitoring mechanisms.
  - Also substituting state-controlled marine police with a central force ignores structural impediments, such as the lack of local intelligence and regional language skills as well as turf wars between the two.
- **Inadequate patrolling:** A **cumulative shortfall (over 90 percent) in the patrolling efforts**, especially at night and decline in physical checks on fishing vessels by the Coastal Police.

**Way forward**

- **Stronger involvement of coastal police:** State police agencies may be integrated in the detection and capture of criminals at sea leveraging their unique access to fishermen and local communities, facilitating the flow of vital human intelligence.
- **Need for a legislative framework**: Comprehensive legislations must be enacted to place systems and processes for the protection of India's maritime infrastructure, covering both the shipping and port sectors.
- **Strengthening of the Coast Guard (CG):** The CG must be strengthened by removing all ambiguities from the Coast Guard Act. There should be a clear command chain and defined standard operating procedures with reference to coastal security.
- **National Commercial Maritime Security Policy Document**: The government must promulgate a National Commercial Maritime Security Policy Document, to articulate its strategic vision for Commercial maritime security.

**Other changes after 26/11 attacks**

- **Intelligence Overhaul:**
  - **National Intelligence Grid (NATGRID)** was constituted to link all governmental databases into create single source of comprehensive intelligence to be accessible to all agencies. It would allow agencies to scan & assess voluminous amount of collected information strategically and identify valuable intelligence leads.
  - **Multi Agency Centres (MACs)** under Intelligence Bureau were strengthened to act as intelligence "fusion-centres" and provide real time 24X7 actionable intelligence.
  - Indian Navy constituted **Joint Operations Centre** to keep vigil over India's extended coastline.
- **Investigation Reforms:**
  - **National Investigation Agency** was setup in **2008** as a **specialized statutory agency** to deal with terrorist offences, without requiring specific consent of the states to take up the cases. Special NIA courts were setup for fast-tracking cases related to terrorism.
  - The **amended Unlawful Activities Prevention Act (UAPA)** has given new powers to the security agencies, including the ability to hold terror suspects for 6 months without charges.
- **Response preparedness:**
  - The **deployment** of the **National Security Guard (NSG)** has also been **decentralized** with **4 new operational hubs** for the NSG to ensure rapid response to terror attacks.
  - **Elite commando force called 'Force One'** was instituted by Maharashtra government with specialized training in line with the National Security Guards (NSG), as per the **recommendations of Ram Pradhan Committee**.

## 2.2. REGIONAL MIGRATION IN INDIA AND SECURITY ISSUES

### Why in News?

Recently, Supreme Court held that a Foreigners' Tribunal's order declaring a person as an illegal migrant would be binding and prevail over the government decision to exclude or include the name from the National Register of Citizens (NRC) in Assam.

**About Foreigners' Tribunals**

- Foreigners' Tribunals (FTs) are **quasi-judicial** bodies meant to determine whether a person is or is not a foreigner under **Foreigner's Act, 1946**.
- FTs were **first setup in 1964** and are **unique to Assam**. In rest of the country, a foreigner apprehended by the police for staying illegally is prosecuted in a local court and later deported/put in detention centres.
- Earlier, powers to constitute tribunals were vested only with Centre. Recently amended **Foreigners (Tribunal) Order, 2019** has empowered district magistrates in all States & Union Territories to set up tribunals to decide whether a person staying illegally in India is a foreigner or not.

**National Register of Citizens (NRC)**

- It is a **list of all bona fide Indian citizens of Assam**, the only state with such a document.
- The NRC is being updated as per **the provisions of The Citizenship Act, 1955 and The Citizenship (Registration of Citizens and Issue of National Identity Cards) Rules, 2003**
- It will **include persons whose names appear in any of the electoral rolls upto the midnight of 24th March, 1971 or National Register of Citizens, 1951 and their descendants.**
- The process of verification involved house-to-house field verification, determination of authenticity of documents, family tree investigations in order to rule out bogus claims of parenthood, and linkages and separate hearings for married women.

### Background

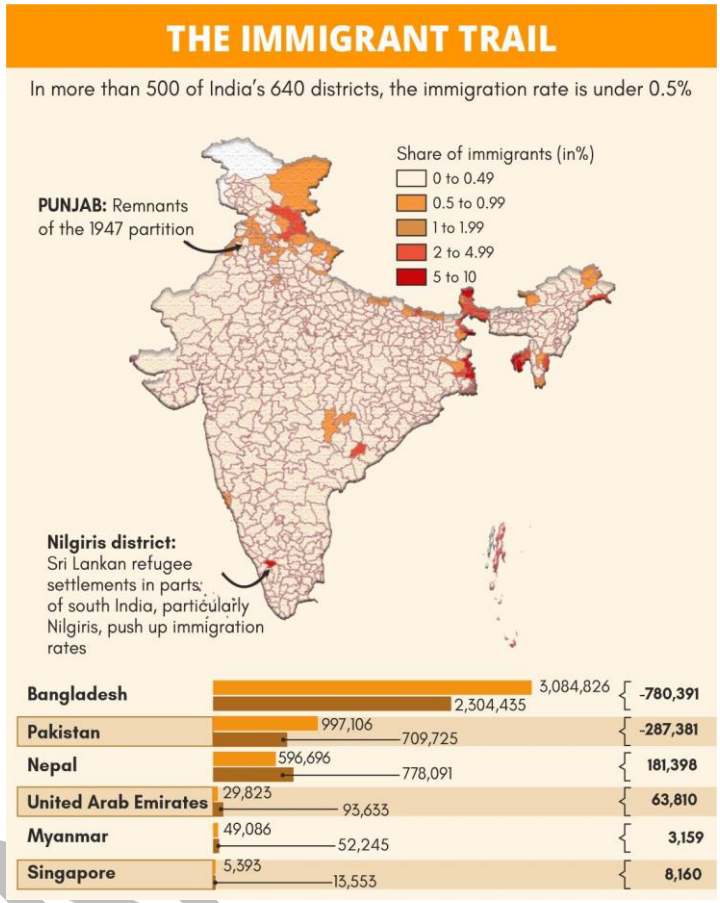
- To tackle the illegal immigration issue just after the independence, NRC was first prepared for Assam after the Census of 1951. But this process rendered ineffective due to vote bank politics.
- In 2014, the Supreme Court asked the state government to update the 1951 NRC in a time-bound manner. Present exercise is being conducted under the supervision of the Supreme Court.
- When the draft NRC was published in 2018, around **40.7 lakh people were excluded** from the NRC. Once the final NRC is published, those excluded can approach **Foreigners' Tribunal**.

### Migration and security

- **Contributory factors of illegal migration**
  - **Increasing pressure on land and mounting unemployment in Bangladesh** due to steep rise in population.
  - **Porous India-Bangladesh border** of 4,096 kms, the fencing of which has not been completed so far.
  - **Better economic opportunities across the border.**
- **Security challenges**
  - **Illegal voters:** Most of the Bangladeshi immigrants have got their names enlisted in the voting list illegally, thereby claiming themselves as citizens of the state.

- ✓ Though there is no evidence to suggest that migration plays a significant role in national elections, it remains a high priority for border states like Assam and serves as a powerful symbol for mobilizing support in state and local politics.

- **Issue of terrorism:** Pakistan's ISI has been active in Bangladesh supporting militant movements in Assam. It is alleged that among the illegal migrants there are also militants, who enter into Assam to carry out the terrorist activities.
  - ✓ By invoking migration as a threat to national identity and societal security, state and non-state actors risk turning what is mostly a social and political issue into a security problem.
  - ✓ In doing so, they deprive migrants-and citizens- of fundamental rights and expose an already vulnerable population to xenophobia.




- **Local Tensions:** Sometimes Migration escalate into political violence and directly impinge on state security
  - ✓ The failure of government to respond to issue of illegal migration led to the agitation by the Assamese and resulted into Assam accord of 1985.

**Options for India**

- **Diplomatic Effort:** India has to make diplomatic effort to get Bangladesh to cooperate as illegal migration cannot be solved unless origin country cooperates. Sharing of digital database of its citizens will make it easier.
- **Better Border Management:** Fencing, construction of border roads and proper management of border will make a difference. Like engaging in proactive patrolling of the India-Bangladesh and India-Myanmar international borders.
- **Unique Identification Number (UID) scheme:** Compilation of data is likely to reduce the comfort level of fresh illegal migrants.
- **Bar from Voting rights:** Bangladeshi who are already in could be allowed to work but should not be allowed to vote and this will diminish their ability to influence government decisions by being a political force.
- **Use of regional forums**: Forums like BIMSTEC can be used to discuss issues like illegal migration from neighbouring countries and garnering support and coordination from the members.
- **Bilateral talks**: India should still seek to engage both Bangladesh and Myanmar to find a resolution to the current humanitarian crisis.

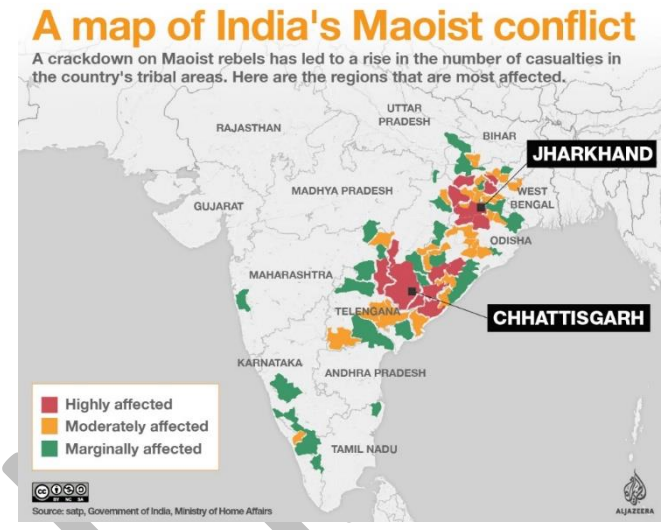
# 3. EXTREMISM

## 3.1. NAXAL VIOLENCE IN INDIA

**Why in News?**

The IED blast that claimed the lives of 15 security personnel and their driver in Gadchiroli, Maharashtra is a grim reminder of the challenge the Naxal movement continues to pose to the country's internal security.

**Left Wing Extremism (LWE) in India**




- The Naxal insurgency in India **originated in a 1967 uprising** in Naxalbari, West Bengal by the Communist Party of India (Marxist). They are the group of people who believe in the political theory derived from the teachings of the **Chinese political leader Mao Zedong.**
- The Naxalites claim to represent the most oppressed people in India, those who are often left untouched by India's development and bypassed by the electoral process
- The conflict is concentrated the Eastern part of the country, particularly an area known as the **Red Corridor** spread across the states of Chhattisgarh, Odisha, Jharkhand, Bihar and Andhra Pradesh.
- It aims to overthrow the government through people's war.
- It creates conditions for non-functioning of the government and actively seeks disruption of development activities as a means to achieve its objective of 'wresting control'. It spreads fear among the law-abiding citizens.
- The problem of LWE or Naxalism in India continues to rank high in the list of internal security challenges that the country faces. But past few years have seen a **considerable improvement in the LWE scenario**.
    - The total number of violent incidents of LWE has **drastically reduced from 1048 in 2016 to 908 in 2017**.
    - The related deaths have seen a 34% decline in 2017 as compared to 2013 indicating success of government efforts.
    - Compared to 2013, surrenders by LWE cadres have increased by 411 percent in 2016.
    - There has been a 43% reduction in casualties to Security Forces personnel.
    - MHA has also **recently redrew the red corridor** by bringing down the number of districts affected with Naxal violence from 106 to 90, spread across 11 states and worst-affected district to 30 from 36.
    - Chhattisgarh, Jharkhand, Odisha and Bihar are declared severely affected by LWE.
    - **The prime criteria** for removing the districts and including new ones was **"Incidents of violence".**
- **Reasons for decline in violence**
    - greater presence of security forces across the LWE affected States.
    - loss of cadres/leaders on account of arrests, surrender and desertions.
    - Rehabilitation program of government
    - better monitoring of development schemes in affected areas
    - insurgency fatigue among the Maoist cadres.
    - shortage of funds, arms and ammunitions.
- However, the LWE are targeting new States and are trying to carve out the base at the tri-junction of Karnataka, Kerala and Tamil Nadu.
- **Urban naxalism** is also posing threat. It is an old Maoists strategy to focus on urban centres for leadership, organise masses, build a united front and engage in military tasks such as providing personnel, material and infrastructure.
- Both the Maoist rebels and the security forces seem engaged in a cycle of violence, with **ordinary citizens caught in the middle**, suffering losses of lives, livelihoods, and living in an atmosphere of fear and intimidation.

**Causes for Spread of Left Extremism**

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

**Important Initiatives for LWE affected states**

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

**SAMADHAN**
It is a strategy of MHA to frame short term and long-term policies to tackle LWE. It includes:
**S**- Smart Leadership
**A**- Aggressive Strategy
**M**- Motivation and Training
**A**- Actionable Intelligence
**D**- Dashboard Based KPIs (Key Performance Indicators) and KRAs (Key Result Areas)
**H**- Harnessing Technology
**A**- Action plan for each Theatre
**N**- No access to Financing

- **National Policy and Action Plan** implemented by MHA since 2015 is a multi-pronged strategy in the areas of security, development, ensuring rights & entitlement of local communities etc. to combat Left Wing Extremism (LWE).
- **Major Sub –Schemes under Scheme Modernization of Police Forces for 2017-20**
  - **Security Related Expenditure (SRE) Scheme (approved in 2017):** aims at strengthening the capacity of the LWE affected States to fight against the LWE problem in an effective manner.
  - **Special Central Assistance (SCA) for 35 most LWE affected districts.**
  - **Special Infrastructure Scheme (SIS)** including construction of 250 Fortified Police Stations in LWE affected states.
  - **Assistance to Central Agencies for LWE management Scheme**
  - **Civic Action Programme (CAP)** to bridge the gaps between Security Forces and local people through personal interaction.
  - **Media Plan Scheme:** to counter the Maoist propaganda.
- **Infrastructure development initiatives**
  - **Road Requirement Plan-I (RRP-I)** is being implemented by **Ministry of Road Transport & Highways,** since 2009 for improving road connectivity in 34 LWE affected districts of 8 States.
  - **Road Connectivity Project for LWE affected areas (RRP-II):** It was approved in 2016 for further improving road connectivity in 44 districts of 9 LWE affected States. **Ministry of Rural Development** (MoRD) is the nodal Ministry for this project.
  - **LWE Mobile Tower Project** to improve mobile connectivity in the LWE areas.
  - **Approval of Projects under** Universal Service Obligation Fund (USOF) supported scheme to provide mobile services in 96 districts of LWE-affected states.
  - **The National Technical Research Organization (NTRO)** is assisting the Security Forces in anti-Naxal operations by providing Unmanned Aerial Vehicles (UAVs).

- **Skill Development related Schemes**
  - **ROSHNI** is a special initiative under, Pandit Deen Dayal Upadhyaya Grameen Kaushalya Yojana which envisages training and placement of rural poor youth from 27 LWE affected districts.
  - **Skill Development in 34 Districts affected by Left Wing Extremism"** under implementation from 2011-12 aims to establish ITIs and Skill Development Centres in LWE affected districts.
- **Surrender and rehabilitation policies:** State Governments have their own policy, while the Central Government supplements the efforts of the State Governments through the Security Related Expenditure (SRE) Scheme for LWE affected States. Additional incentives are given for surrendering with weapons/ammunition. The surrenderees are also imparted vocational training with a monthly stipend for a maximum period of 36 months.
- **Institutional measures**
  - **Black Panther combat force -** A specialised anti-Naxal combat force for Chhattisgarh on the lines of Greyhounds unit in Telangana and Andhra Pradesh.
  - **Bastariya Batallion –** A newly formed batallion of CRPF with more than 534 tribal youth from four highly naxal infested districts of Chhattisgarh along with adequate female representation in sync with the Government's policy of 33% reservation for women making it the first composite battalion in any of paramilitary forces.
  - A process has also been initiated to create a **separate vertical in the NIA** for investigating important cases relating to Left Wing Extremism (LWE)
  - **Multi-disciplinary groups to check funding of Naxalites -** Union ministry of home affairs has formed multi-disciplinary groups with officers from central agencies, including from the IB, NIA, CBI, ED and DRI, and state police to choke the financial flow to Maoists.
- **Constructively engaging youth through education**: Seeing the success of educational hub and a livelihood centre in Dantewada district, the government has now opened up livelihood centres, known as Livelihood Colleges, in all the districts.
- **Other measures**: More bank branches have been opened to ensure financial inclusion. All India Radio stations in the three southern districts of Bastar will now broadcast regional programmes to increase entertainment options. And a new rail service in Bastar is set to throw open a new market for wooden artefacts and bell metal.

**Issues in handling LWE**

- **Negligence of established standard operating procedures** at times leads to loss of valuable lives of security personnel.
- **Certain vulnerabilities** remain such as poor planning, inadequate numbers, insufficient intelligence backup etc.
- **Structural deficits and deficiencies** such as putting IPS deputationists into almost every senior position in CRPF ignoring the decades of experience within the Force.
- **Sluggish Capacity building of police forces,** for example – in Chattisgarh, there are about 10,000 vacancies in different ranks in state police and 23 sanctioned police stations have yet to be set up.
- LWEs are well trained in guerilla warfare.
- **Inefficient technology of mine detection**: Present technology is unable to detect deep planted mines under the road.
- **Delay in acquisition of technology**: For example- Out of the 157 sanctioned MPVs, only 13 have been supplied by OFB to CAPFs so far.
- **Laundering of funds:** Naxal leaders operating in Bihar and Jharkhand are laundering extorted money through acquiring movable and immovable assets.

**Way forward**

- **Learning from Chattisgarh police**: As the Chhattisgarh police have experience in tackling Maoists in Bastar, they are now coordinating with the bordering States to strengthen intelligence and ground presence. Such measures can be taken in new areas as well where Maoists are trying to establish themselves.
- **Eliminating the root cause of the problem** that is leading to the alienation of tribals in this area. The focus should now be on building roads, increasing administrative and political access of the tribals, improving reach of government schemes etc.

- **Centre-state cooperation:** Centre and states should continue with their coordinated efforts where Centre should play a supportive role with state police forces taking the lead.
- **Undertaking technological solutions:** such as use of micro or mini-UAVs or small drones to minimize loss of lives of security personnel.
- **Build trust:** Winning a psychological war against the Maoists remains an unfinished task. To bridge this trust deficit, civil society must join hands with the government in realising the villagers' right to development.
- **Awareness generation:** Government should undertake awareness and outreach programmes and inclusive developmental programmes.
- **Forest Rights**: Effective implementation of the Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Rights) Act, 2006
- **Financial empowerment:** Introduce measures to encourage formation of 'Self Help Groups' (SHGs) to improve access to credit and marketing and empower the disadvantaged.
- **Choke funding**: The nexus between illegal mining/forest contractors and transporters and extremists which provides the financial support for the extremist movement needs to be broken through establishment of special anti-extortion and anti-money laundering cell by State Police.
- **Infrastructure development**: For implementing large infrastructure projects, particularly road networks that are strongly opposed by the extremists need to be undertaken with the help of specialised Government agencies like the **Border Roads Organisation** instead of local contractors.
- **Special efforts are needed to monitor the implementation** of constitutional and statutory safeguards, development schemes and land reforms initiatives for containing discontent among sections vulnerable to the propaganda of violent left extremism

The **two-pronged policy** of direct action by the security forces combined with development is showing results — the government has already made a dent in most of the affected districts and is determined to check the expansion of Maoists. The paradigm of **proactive policing and holistic development** should ensure more such significant results in the future.

## 3.2. CROSS-BORDER LINKAGES IN NORTHEAST INSURGENCY

**Why in News?**

The armies of **India and Myanmar** carried out a coordinated operation named **Operation Sunrise 2** in their respective border areas, targeting several militant groups operating in **Manipur, Nagaland and Assam**.

**About Operation Sunrise 2**

- The armies coordinated with each other to bust camps of militant outfits, including the **Kamtapur Liberation Organisation, the National Socialist Council of Nagaland (Khaplang), the United Liberation Front of Assam (I) and the National Democratic Front of Boroland.**
- The **first phase of "Operation Sunrise"** was conducted **in February 2019** along the Indo-Myanmar border, during which a number of camps **of north-east-based militant groups were busted.**


**Background**

- 90% of the **North-East is contiguous with the international border**, which allows terror outfits to get sanctuaries in **Bhutan, Myanmar, Bangladesh and even China and Nepal.**
- The insurgent groups started developing their **international linkages immediately after the independence in 1947.**
- India's 5,800-km long land border with Myanmar and Bangladesh extends across **Assam, Tripura, Mizoram, Meghalaya, West Bengal, Nagaland, Manipur and Arunachal Pradesh**. All these States have faced, or continue to face, **trans-border terrorist and separatist challenges.**

**Reasons for cross border insurgency**

- **Safe Havens:** The shelter and support that the Indian insurgent groups receive from across the border have been one of the most important factors which has helped them in sustaining their rebellion.
- **Economic support:** The Golden Triangle (comprising Myanmar, Laos and Thailand) has provided an economic boom for the insurgent groups to sustain themselves.
- **Availability of weapons:** Easy availability of small arms in neighboring countries like Bangladesh and Myanmar has been another factor behind the sustenance of insurgency in the region.
- **Ethnic affinity:** Many ethnic groups in the region, especially in the areas bordering the international boundaries, have more in common with the population living across the boundary than with their own nationals.
- **Border issues in North east**
    - **Terrain of Border:** Difficult terrain along border with different countries in north east make means of transportation and communication difficult and as a result, the border area remains sparsely populated with depressed economic development.
        - ✓ **High mountains, deep river channels** together with lush forest characterize the borderland with Myanmar.
        - ✓ **Inaccessible forested areas** along the Assam– Bhutan border continue to serve as temporary bases and safe havens for the insurgent groups.
        - ✓ **River line borders in Bangladesh** tend to change course periodically, leading to a host of disputes associated with the difficulties in establishing ownership of the newly created territories.
    - **Boundary issue:** Even though the international boundary between countries like India and Myanmar had been formally delimited and demarcated following the boundary agreement in 1967, the boundary has not crystallised on the ground as lines separating two sovereign countries.
    - **Free movement regime:** India-Myanmar border has a unique arrangement in place called the Free Movement Regime (FMR). The FMR permits the tribes residing along the border to travel 16-km across the boundary without visa restrictions.

**Way Forward**

- **Sensitization of people**: The border community should be sensitised to participate in the nation building project through sustained community interaction programmes**.**
    - Increase cultural exchanges, tourism and people-to-people contact, including provision of job permits and work visas, for the South Asian countries.
- **Cooperation with neighboring countries**: International borders are best managed when neighbours cooperate to secure their mutual borders. For such cooperation to materialise, political and diplomatic initiatives are required to be carefully crafted**.**
- **Strengthening of Regional Forums:** Regional groupings like SAARC, BIMSTEC, BCIM can help in enhancing economic and security cooperation with these countries which will lead to a better understanding of benefits of peace in North-East India.
- **Effective Border Management through 'smart borders** which ensure quick and easy, legal flow of people and goods, while maintaining a steady momentum in the process of improvement of infrastructure and other facilities at checkpoints.
- **Joint Training and operations:** Exercises like **"Hand in hand"** with China, **"Operation Sampriti"** between India and Bangladesh etc. can help to combat terrorism.
    - **'Operation All Clear'** by Bhutan was a landmark operation which was conducted against Assam separatist insurgent groups in the southern regions of Bhutan.

# 4. ROLE OF EXTERNAL STATE AND NON-STATE ACTORS

## 4.1. TECHNOLOGY AND EXTREMISM

**Why in News?**

The livestreamed killing of people in Christchurch, New Zealand, has thrown a spotlight on how terrorists are using technology for their end.

**Background**

- The modern terrorism is instantaneous and unpredictable, a global threat that hit its targets, but at same time **hits a wide audience due to use of technology.**
- Terrorists have been **using cyberspace to find resources, make propaganda activities** and from which it is possible to launch the attacks against enemies everywhere in the world.
- **Social media** is **an essential element of modern terrorism**; these powerful platforms allow terrorists to **communicate**, to make **propaganda** and **recruit** new sympathizers at the same time maintaining anonymity to the user.

**How technology is being used in propagating extremism?**

- **Propaganda:** It generally takes the form of multimedia communications providing ideological or practical instruction, explanations, justifications or promotion of terrorist activities. It is being used for promotion of violence, recruitment, incitement and radicalization.
- **Financing:** Online payment facilities offered through dedicated websites or communications platforms make it easy to transfer funds electronically between parties. Financial support provided to seemingly legitimate organizations, such as charities, may also be diverted for illicit purposes.
- **Training:** Instructional material are being made available with use of technology which imparts training and facilitate online counter-intelligence and hacking activities.
- **Planning:** Technology also facilitates the preparation of terror activities thorough communication channels , both within and between the terror outfits located in different geographies.
- **Execution:** Internet communications may also be used as a means to coordinate the execution of physical acts of terrorism.
- **Cyber attacks:** These attacks are typically intended to disrupt the proper functioning of targets, such as computer systems, servers or underlying infrastructure.

**Strengthening technological framework to counter extremism**

- There is need for government and online service providers to take collective initiative to combat online extremism and secure the Internet. For e.g. recently, a document called **"Christchurch Call to Action"** was signed and adopted with participation from 26 nations, including India. It provides following measures:
- **Role of Online service providers**
  - **Terms of Use:** Updating terms of use, community standards, codes of conduct, and acceptable use policies to expressly prohibit the distribution of terrorist and violent extremist content.
  - **User Reporting of Terrorist and Violent Extremist Content:** Providing easy to use methods within online platforms and services for users to report or flag inappropriate content.
  - **Enhancing Technology:** Prevent the **upload & dissemination** of terrorist and violent extremist content, with a **mechanism for automatic identification** and immediate & permanent removal.
  - **Transparency Reports:** Publishing on a regular basis transparency reports regarding detection and removal of terrorist or violent extremist content on online platforms
- **Role of Government and civil society**
  - **Shared Technology Development:** Share technology with other industries, governments, and NGOs, such as data sets and open source content AI detection tools.
  - **Crisis Protocols:** Creating a crisis protocol for responding to emerging or active events, on an urgent basis, so relevant information can be quickly and efficiently shared, processed, and acted upon by all stakeholders with minimal delay.

- **Education:** Collaborate with industry, governments, educational institutions, and NGOs to help educate the public about terrorist and extremist violent content online & how to report it.
- **Work together** to ensure cross-industry efforts are coordinated and robust and coordinate with Governments and civil society. E.g. Investing in and expanding the **GIFCT**
  - ✓ **Global Internet Forum to Counter Terrorism (GIFCT)** is an industry led initiative, working in close partnership with the UN Counter Terrorism Executive Directorate (UNCTED) to substantially disrupt terrorists' ability to promote terrorism, disseminate violent extremist propaganda.
- **Combating Hate & Bigotry: Support research and academic efforts** to better understand and attack root causes of extremism and supporting capability and capacity of NGOs to promote pluralism.

**Christchurch Call To Action**

- It outlines **collective, voluntary commitments from governments and online service providers** intended to address the issue of violent extremist content online and to prevent abuse of the internet, while maintaining international human right laws.
- **Under the Call, the Governments have committed to:**
  - **Counter drivers of terrorism and violent extremism** by strengthening resilience and inclusiveness of societies.
  - Ensure **effective enforcement of laws**.
  - Encourage **media outlets to apply ethical standards** when depicting terrorist events online.
  - **Awareness-raising and capacity-building** of smaller online service providers,
  - development of industry **standards or voluntary frameworks**
  - policy measures to prevent dissemination of extremist content, while maintaining free, open and secure internet.
  - **Ensure appropriate cooperation with and among law enforcement agencies**.

## 4.2. CHALLENGE OF ISIS IN INDIA

**Why in news?**

Recently, the Islamic State (IS) terror group has claimed for the first time that it has established a **"province"** in India, after a clash between militants and security forces in the Kashmir region killed a militant with alleged ties to the group.

**Background**

- **Islamic state** previously known as the **Islamic state of Iraq and Syria (ISIS)**, is a terror group which envisages to establish an **"Islamic state based on Sharia law or Islamic Caliphate"**.
- IS's **Amaq News Agency** has announced its new province in India, that it called **"Wilayah of Hind"**, but did not elaborate on the branch's geographical remit.
- In the past, IS had vowed to convert India into **Khurasan State,** a historic name for a region that covers Afghanistan, Pakistan, parts of India, and other surrounding countries**.**

**Why Islamic State is a challenge for India?**

- **Involvement of other state actors-** such as Pakistan's Inter-Services Intelligence (ISI), which can provide a well-established intelligence and logistic network, in a symbiotic relationship. The NIA reported in 2014, the recruitment of more than 300 Indian youths by Pakistan-based Tehreek-e-Taliban (TTP), which had joined hands with ISIS.
- **IS losing territorial ground in other areas-** such as Middle East to US-led forces, now IS is seeking to strengthening its global affiliations. Such a strategy was highlighted by ISIS chief Abu Bakr al-Baghdadi in the past. At the same time, ISIS views India as a potential hotbed for radicalization due to the demographic structure.
- **Efforts of radicalization-** The IS have published recruiting materials in Hindi, Urdu, Tamil and other languages spoken in India. In 2015, it released an e-book to spread its propaganda and making direct reference to Indian Prime Minister accusing him of spreading communal disharmony. So far, India has had some 82 active cases of investigations on individuals suspected of engaging in pro-ISIS activities.

**Strengths of India in the fight towards IS**

- Despite the initial euphoria, ISIS has not been able to create much of an influence in India.
- Recently, more than 1,000 Muslim leaders in India issued a fatwa condemning the terror group **as "un-Islamic and inhuman."**

- The majority of the Muslims in India have historically followed a **liberal and spiritual faith of Islam** -- which is not based on the outer trappings of Islam but focused on the inner essentials of the religion.
- Over the centuries of co-existence and cultural intermingling, there emerged a mixed and mosaic-like Hindu-Muslim culture in the **Indo-Gangetic (popularly known as Ganga-Jamuni Tehzeeb).**
- The fertile grounds of recruitment which ISIS finds in Europe are not present in India. Many of the ISIS cadres from Europe are drug-addicts, new converts and youth suffering from depression; many of them lack a social support system and have weak family ties and feel the effects of cultural deracination.
- Also, more or less, the constitutional fundamental rights mandated to all citizens of India given every citizen a sense of confidence.

**Related News - Al Qaeda released maiden video on Kashmir**
Even though Al Qaeda- has been active in the Indian subcontinent (Al Qaeda in the Indian Subcontinent (AQIS) was founded in 2014), it has largely been unable to carry out large-scale attacks and struggled to attract support outside of Pakistan.
Reasons for the new-found interest of Al Qaida in India:
- **The aging leadership of Al Qaida is struggling to compete with the IS** for young radicalized recruits. As IS remain majorly involved in West Asia, **it suits to the Al Qaeda's strategy to "invest" in the East**.
- Another reason is due to the fact that India has substantially increased its engagement with Afghanistan since the fall of the Taliban government. So, **India's growing influence may deter Al Qaida's re-emergence** to power in Afghanistan.

**Vulnerabilities of India**

- **Gaps in intelligence architecture-**
  - The Intelligence Bureau (IB), the designated premier agency, is hamstrung by inadequate manpower and equipment.
  - The National Investigative Agency (NIA) established in 2008 to exclusively investigate terror cases, lacks muscle, and receives little cooperation from state police forces which resent its intrusion.
  - The Defence Intelligence Agency (DIA) was set up in 2002, but is underutilised in the absence of a chief of defence staff, and duplicates the external intelligence work being done by the Research & Analysis Wing (RAW).
- **Inadequate technical research capacity-** The National Technical Research Organisation (NTRO), failed to flag twitter accounts such as ShamiWitness, which allegedly became one of the most vocal proponents of ISIS on the Internet. The NatGrid, a national, computerised information sharing network, which was first mooted in 2001 but did not see the light of day till 2008, is still struggling to become fully operational.
- **Radicalization emanating from the neighbourhood-** There have been examples of Bangladeshi and Indian pro-ISIS individuals attempting to work together online to form a larger base of like-minded individuals to create an organised entity.
- **Presence of other terror groups-** With the dismantling of the Indian Mujahideen, several radical extremists groups are looking for an alternate identity and ISIS may well provide the much desired character.
  - The appearance of black flags in Jammu and Kashmir preceding the Indian PM's visit was one such instance where local insurgent outfits were using the name of ISIS in order to garner attention**.**

**Way Forward**

- **A 360- degree approach:** It is necessary for India to effect changes in its internal security architecture and further empower its intelligence and investigation agencies for enhanced preparedness, along with some diplomatic measures to counter terrorism in the whole of the sub -continent.
  - **Cross platform recruitment of specialists** dealing with social media, big data analysis, terrorism finance and technical intelligence.
  - Developing a **well-operated online intelligence network** for intelligence sharing, joint online operations and database convergence to keep a check on ISIS's influence on the internet.
- **Early prevention and deradicalisation:** A comprehensive strategy of early prevention, targeted repression and intervention and involves government and non-governmental actors.
  - **Influential Minority Religious leaders** should be roped in to appeal to youth against radical propaganda, especially those coming through social media and other internet platforms.
  - The **government should work with social groups, NGOs and student bodies**, which can reach out easily to the population at large, as compared to state institutions.

# 4.3. TERROR ACTIVITIES AND MUTUAL DISTRUST IN INDIA-PAKISTAN RELATIONS

**Why in news?**

The recent terror attack on Indian security forces in Pulwama led to the India-Pakistan tensions on an all time high in the near past.

**Background of Terrorism in India-Pakistan Relations**

- Stemming from the **two-nation theory** of Pakistan, the conflict of control over Jammu and Kashmir (Muslim Majority State) has led to multiple wars and skirmishes between the two countries.
- But, this two-nation theory was debunked after **1971**, when Bangla speaking Muslim population formed a new country of **Bangladesh**.
- After 1971, Pakistan changed the course. This **military incapacity** of Pakistan, led it to change the course in fighting an **asymmetric warfare** against India. The Pakistani deep state (The Army and the ISI) nurtured **terror as a state policy** to deal with India.
- This policy has resulted in a **mutual distrust** between the two nations.
- Whenever, the governments of two nations have tried to indulge in confidence building measures (Bus Diplomacy, Sports, Summits, Kartarpur Corridor), the cross border terror activities have derailed such Indo-Pak dialogue.

**Terror as a State Policy of Pakistan**

- Deep State is a body of people, typically influential members of government agencies or the military, believed to be involved in the secret manipulation or control of government policy.
- Deep State in Pakistan has nurtured Islamic Radical Groups (**Mujahideens**) as strategic assets to be used against its adversaries.
- This strategy was increasingly adopted after the success of US-funded Mujahideens in Afghanistan against USSR.
- There are primarily three types of such groups-
  - **Ones who act against India**- e.g. Lashkar-e-taiba, Jaish-e-mohammed
  - **Ones who act against Afghanistan**- e.g. Al-Qaeda and Taliban
  - **The Pakistani Taliban** (Tehreek-e-Taliban-Pakistan)- this group has become rogue and fighting against the Pakistani establishment itself.
- **Lack of Terror Crackdown**- Pakistan has remained in denial mode and taken sham actions on its terror assets to avoid international pressure.
- Also, Pakistani State does not have the capacity to deal with them militarily, if armed rebellion takes place since these groups have certain constituency in Pakistan.

**Measures taken by India to deal with Pak- sponsored terrorism**

- **Military Efforts-** India has conducted strikes on terror camps in 2016 and 2019. Also, the state has launched the **Mission All Out** to liquidate all the terrorists in the Jammu and Kashmir.
- **Economic Efforts-** the Indian government has withdrawn **"Most Favoured Nation"** or MFN status accorded to Pakistan.
- **Strategic Shift-** India made an unprecedented direct reference to Baloch freedom struggle in the PM's Independence Day speech.
- **Diplomatic Efforts-**
  - All major countries including America, Russia, France, U.K and Australia have supported India on its counter-terror activity. Recently, Saudi Arabia and Organization of Islamic Countries also supported India's stand on terror.
  - India has started to completely utilize its share of water under the Indus Water Treaty, by building dams in Jammu and Kashmir.
  - In 2016, after the Uri Attack, India successfully isolated Pakistan in the 19th SAARC summit. Since then, no SAARC meeting has happened.
- **International Measures on Terrorism-** India has been pushing for the adoption of universal definition of terrorism and steps needed to tackle it under the **Comprehensive Convention on International Terrorism (CCIT).**

**Change in Indian approach towards Pak-based terror**

- On 14th February, 2019- a vehicle bound suicide attack led to **death of 40 CRPF personnel in Pulwama, Jammu and Kashmir**.
- The links to this attack were again traced to Pakistan based terror group **Jaish-e-Mohammed**.
- On 26th February, the Indian Airforce hit a training camp of the group in **Balakot, Pakistan**.
- This marked a change in Indian response, as it was a **pre-emptive strike on non-military, non- civilian target** to fight terror.
- It was a mature decision to achieve the target, as well as, prevent any escalation towards war.

- **Setting up of a Multi-disciplinary terror monitoring group (MDTMG):** to ensure synergised and concerted action against terror financing and terror-related activities in Jammu and Kashmir.

**Impact of Pakistan sponsored terror activities**

- **Holdback regional peace and security-** such as recent attacks in India, Afghanistan and Iran. People-to-People Contact remains low and the region has become a hotbed for even a nuclear showdown.
- **Roadblock in SAARC and trade**- The South Asian Sub-continent remains deprived of regional trade, market access and prosperity on the lines of European Union and other blocs, due to Pakistan's obstructionism and terror politics.
- **Diversion of resources towards arm procurement**- With both the countries entering into an arms race, resources are diverted which could have been used to address other human demography challenges in the region such as poverty, diseases etc. For instance, in the period of 2000-2016, Jammu and Kashmir got Rs. 1.14 trillion in grants and much of it was used for security.
- **Small constituency being able to hold back majority interests**- which includes Pakistan's deep state and small section in Kashmir Valley that ends up driving the overall discourse in the region.
- **Rising discontent in the region** – due to lack of development in the region which creates a vicious cycle whereby youth from this region becomes more vulnerable towards radicalism.

**Need to take a multi-pronged strategy towards terror infrastructure**

- **To deal with Pakistan based terror-**
  - **Inflict Costs of Terrorism-** A consistent policy must be evolved, where the Pakistan deep state bears the brunt of sponsoring terror against India, as done in recent Air Strikes in Balakot.
  - **Alert Defence Architecture-** Indian defence forces have to keep the tempo up at all levels, be it at the Line of Control, Jammu and Kashmir or any other region.
  - **Declare Pakistan as a Terror State-** to put pressure on Pakistan. Here the need is to take the international community along with India.
  - **Economic Measures-** Pakistan has large foreign debt with a small foreign exchange reserves. If, the FATF further downgrades Pakistan to **black list**, its financial condition will be completely crippled. This pressure must be kept on Pakistan.
  - **Talk with Pakistan's all weather allies-** Need to talk with countries like China, Saudi Arabia, Turkey on India's stand on terror, be it on banning terrorists or working on counter-terror activities.
  - **Cohesive Boycott**- An integrated national response should be given to any terror activity emanating from Pakistan. There should be no soft engagement channels with Pakistan like Bollywood, Sports, Cultural activities.

**Issues in dealing with Pakistan's terror infrastructure**

- It has been difficult to completely isolate Pakistan in the international community for long time, because it has -
  - Large population
  - Nuclear Capabilities
  - Islamic nations backing Pakistan
- The organs of Pakistani state, be it the Executive or the Judiciary or the Civil Society- have been overshadowed by its deep state. Whenever in the past, any of the other organs tried to stand, they have been crippled by the deep state.
- The illness of its Deep State run so deep, that it has become incurable. If nuclear weapons come in the hands of Terror groups, it may become a danger for international peace.

- **To improve India's counter-terror capabilities-**
  - **Kashmir Outreach-** Further increase the democratization process, employment opportunities under schemes like Udaan, talks with radicalized youth.
  - **Intelligence Gathering-** Need for comprehensive intelligent reforms with focus on creating synergies among various agencies, forces and people.
  - **NCTC-** Consensus needs to be formed on **National Counter Terrorism Centre**, which will work as an federal anti-terror agency, as proposed after 2008 Mumbai attacks.
  - **De-radicalization-** Given the dangers of ISIS, lone wolf attacks, a national effort on de-radicalization needs to be taken up. Some states like Maharashtra, Karnataka have taken some steps in this direction.
  - **Hit Terror Financing-** All sources of money, which are used to fund terror activities, need to be dried. Actions such as recent crackdown on Jamaat-i-Islami could be done on other such organizations found in this regard.

# 4.4. GLOBAL COORDINATION FOR COUNTERING TERRORISM

**Why in News?**

Recently, UN launched a new framework **"UN Global Counter-Terrorism Coordination Compact"**.

**Need for global coordination**

- **Changing face of terrorism leading to global diffusion of threat:** In recent years, terrorist networks have evolved, moving away from a dependency on state sponsorship; many of the most dangerous groups and individuals now operate as non-state actors.
  - While some remain focused on local or national political dynamics, others seek to affect global change.
  - Lack of a universal agreement over what constitutes terrorism weakens efforts to formulate a concerted global response.
- **Fragmented approach:** Multilateral action suffers from inadequate compliance and enforcement of existing instruments.
  - With a global counterterror co-operation mechanism, the actions of uncooperative states could be addressed and scapacity-building efforts—currently scattered across bilateral and multilateral relationships—could be brought under a single structure.
- **Porous borders and interconnected international system:** Taking advantage of porous borders and interconnected international systems—finance, communications, and transit—terrorist groups can operate from every corner of the globe. Nonstate actors that can easily cross borders and operate in civilian areas poses an enormous challenge.
- **Incapacity of countries to control terrorist threats:** Multilateral initiatives bolster state capacity to build institutions and programs that strengthen a range of activities, from policing to counter radicalization programs.
- **Emerging challenges: Vigilance against misuse of emerging technology** such as artificial intelligence, drones and 3D (three-dimensional) printing, as well as against **the use of hate-speech** and distortion of religious beliefs by extremist and terrorist groups.

**About UN Global Counter-Terrorism Coordination Compact**

It is an agreement between the UN chief, 36 organizational entities, the International Criminal Police Organisation (INTERPOL) and the World Customs Organisation, to **tackle the scourge of international terrorism**.

**Objective**

- To **ensure that the United Nations system provides coordinated capacity-building** support to Member States, at their request, in implementing the UN Global Counter-Terrorism Strategy and other relevant resolutions.
- To **foster close collaboration** between the Security Council mandated bodies and the rest of the United Nations system.
- **UN Global Counter-Terrorism Compact Coordination Committee** will oversee and monitor the implementation of the Compact which will be chaired by UN Under-Secretary-General for counter-terrorism.
- It will **replace the Counter-Terrorism Implementation Task Force**, which was established in 2005

**Global Counter-Terrorism Strategy**

- The United Nations General Assembly (UNGA) adopted it in 2006 and it is a unique global instrument to enhance national, regional and international efforts to counter terrorism.
- UNGA reviews the Strategy every two years, making it a living document attuned to Member States' counter-terrorism priorities.
- The **four pillars of the Global Strategy** include:
  - Measures to address the conditions conducive to the spread of terrorism.
  - Measures to prevent and combat terrorism.
  - Measures to build states' capacity to prevent and combat terrorism and to strengthen the role of the United Nations system in that regard.
  - Measures to ensure respect for human rights for all and the rule of law as the fundamental basis for the fight against terrorism.

**Various Global Actions for countering Terrorism**

- **United Nations** oversees various conventions that target different aspects of terrorism, including terrorist financing, hijacking, acquiring weapons of mass destruction, and hostage taking, to name a few.
  - **UN General Assembly unanimously adopted in 2006 the Global Counterterrorism Strategy (GCT).**
  - **Counterterrorism Implementation Task Force (CTITF)**—a partnership of bodies created by UN in 2005, which now includes more than thirty UN entities plus INTERPOL, to streamline and coordinate counterterrorism efforts within the UN.
  - **UNSC** established the **Counterterrorism Committee (CTC)**
  - **Terrorist Travel Initiative** was launched under auspices of Global Counterterrorism Forum (GCTF).

- ✓ It will bring together national and local governments, law enforcement and border screening practitioners, and international organizations to share expertise on how to develop and implement effective counterterrorism watch listing and screening tools.
- ✓ The initiative will a develop set of good practices which will reinforce countries and organizations to use border security tools prescribed in UNSC Resolution 2396 to stop terrorist travel.

- **Financial Action Task Force (FATF) and the Group of Eight (G8) Counterterrorism Action Group (CTAG)**
- European Union's the **EU judicial cooperation unit, EUROJUST and the EU's police force, EUROPOL.**

**Counter-terrorism - India's involvement at UN**

- India has prioritised the adoption of an **intergovernmental framework** to combat terrorism.
- India introduced the **Comprehensive Convention on International Terrorism** (CCIT) in 1996 that defined terrorism and enhanced "normative processes for the prosecution and extradition of terrorists."
- Active participation in several counter-terrorism discussions, such as
  - **drafting a Global Counter-Terrorism Strategy** in the General Assembly in 2006,
  - serving as a founding members of the Global Counter-Terrorism Forum (GCTF),
  - supporting counterterrorism mechanisms established by UN Security Council Resolutions, such as Resolution 1373 establishing the Counter-Terrorism Committee, and **Resolution 1540** addressing the non-proliferation of Weapons of Mass Destruction to terrorist organisations.

## 4.5. "LONE WOLF" ATTACKS

**Why in News?**

The Union Home Minister has said that threats posed by "lone wolf" attackers and "do it yourself' terrorists are a major challenge for the security agencies.

**Lone Wolf Attacks**

- A "lone wolf" is a person who prepares and commits violent acts alone, outside of any command structure and without material assistance from any group.
- It is an efficient way of spreading terror in hard-to-access places for organised terrorist groups.
- Prominent recent examples across the globe include Boston marathon bombing of 2013, Sydney hostage crisis of 2014, recent attacks in New York and London where vehicles were used to run over and kill a number of people.

| Conventional terror attacks | Lone wolf terror attacks |
|---|---|
| Mostly multiple perpetrators | Mostly single perpetrator |
| A definite command structure | Lack of hierarchical command structure |
| Family member, social circle, etc. likely to be aware/involved. | Family members are not likely to be aware of the radicalisation of the individual. |

**Causes of Lone wolf Attacks**

- **Alienation of communities:** As communities get isolated and become less trustful of law, they become alienated. It then provides grievances for terrorists to exploit as individuals from such communities tend to easily be self-radicalized by accessing material online.
- **Mental and psychological disorders** can also often be a trigger for carrying out random attacks by individuals.
- **Lax gun control** (for example in USA) create a fertile ground for carrying out of Lone wolf attacks.

**Challenges**

- **Difficult to Apprehend:** Traditional terror groups with command and control "are easier for government to control. "Leaderless Resistance" like lone wolf attacks create an intelligence nightmare.
- **Use of Social Media by terror groups:**
  - Since the IS has been able to successfully recruit Indians via social media for the war in Syria it is a matter of time before they find recruits willing to employ violence in India itself.
  - The head of Al-Qaeda Indian Subcontinent called on Indian Muslims to follow the example of lone wolves in Europe and kill officers in India.
- **Possibilities of a complex Network:** Recent investigations have shown that often these attacks are not entirely independent and leaders operating remotely exercise various degrees of influence, acting as confidants and coaches and coaxing recruits to embrace violence.

**Way Forward**

- **Monitoring of Online content –**
  - Better vigilance regarding online radicalization by terror groups is required to curb this challenge.
  - Big data analytics must be used to discern the level of radicalisation of potential recruits, their networks and sources of information, funding and leadership in order to help unravel the roots of radicalisation.
- **Enhancing Social capital:** Enhancing the "sense of belonging" among different groups rather creating division can be of great impact. For example, preventing polarisation along religious or ethnic lines through effective social integration is needed.
- **Influence of Family and Peer Groups:** It must be utilised by the state to pre-empt any radicalisation of young individuals to any terror group's ideology.
- **Providing access to Mental Healthcare and counselling**: Helplines by professional counsellors to counsel against radicalization once it is reported by some friend or family member.
- **Coordination:**
  - Coordination and intelligence sharing between agencies such as IB, NIA, State police, etc is a must to prevent such incidents.
  - The nature of threat that groups like the IS represent is transnational in nature. Therefore there is also a need to improve intelligence sharing, faster processing of information requests, countering the finance mechanisms, and facilitate easier extradition.
- **Providing training to police personnel:** State police forces should be trained to develop counter-terror capabilities as they are the "first responders" when an attack takes place.

**Lone wolf attacks in India**

- **Volatile neighbourhood of India acting as terror hotbeds, fast growing population** especially youth with access to mass media and social media, **heavy concentration of people in public areas** with limited security and **inadequate capacities of local police** increase India's vulnerability to lone wolf attacks.
- However various other factors tend to pose challenges in growth of lone wolf attacks in India:
  - Unlike in the US where sophisticated weapons can be easily bought by ordinary citizens, gaining access to such weaponry in India is difficult.
  - Indians have not displayed the psychological willingness to undertake high risk attacks.
  - The absence of past examples of lone wolf attacks in India inculcates the fear of the unknown in the minds of potential volunteers.

**Some Steps Taken by India**

- **Education and skilling** - Modernization of madrassas, Employment and skilling schemes for jobless youth like Nai Manzil, Himayat etc.
- **Specific programmes** like 'Operation Chakravyuh' of the IB, where a dedicated set of officers monitor the web, tracing the activities of the youth who are in touch terror operatives.
- **NATGRID** is in the process of being scaled up.
- **National Cyber Coordination Centre (NCCC)** has been established as a cyber security and e-surveillance agency in India.
- **WHAM** (winning hearts and minds) strategy approach by security forces to prevent alienation.
- **Deployment of private security** at high value targets like malls, hotels and schools has been upgraded, which acts as a deterrent to an individual aiming to target them.

## 4.6. ARMED FORCES SPECIAL POWERS ACT (AFSPA)

**Why in news?**

After 32 years of imposition, Armed Forces Special Powers Act (AFSPA) was partially withdrawn from three of the Arunanchal Pradesh's nine districts by Ministry of Home Affairs (MHA).

**About AFSPA**

- Armed Forces (Special Powers) Act, enacted in the year 1958, **grants extra-ordinary powers and immunity to the armed forces** to bring back order in the "disturbed areas".
- Areas are considered disturbed "by reason of differences or disputes between members of different religious, racial, language or regional groups or castes or communities".
- AFSPA **empowers the Governor of the State/Union territory** to issue an official notification declaring the state or a region within as a "disturbed area", after which the Centre can decide whether to send in armed forces.
- Some of these extra-ordinary powers include:

- Fire upon anyone after giving warning who is acting against law & order in the disturbed area.
- Arrest anyone without warrant.
- Stop and search any vehicle or vessel.
- Armed forces personnel have legal immunity for their actions.

- **Presently AFSPA** is enforced in the 5 states of North East (parts of Arunachal, Assam, Manipur, Mizoram & Nagaland) and J&K.

**Rationale behind imposition of AFSPA**

- **Effective functioning:** It is essential for the armed forces to function effectively in insurgency and militancy affected areas.
- **Security of nation:** Provisions of this act have played a crucial role in maintaining law and order in disturbed areas. Thus, protecting **sovereignty and security of the nation**.
- **Protection of member of armed forces:** It is crucial to empower members of armed forces who **constantly face threat** to their lives at the hands of insurgents and militants. Its withdrawal would result in **poor morale**.
  - Extra-ordinary powers are also necessary as the armed forces **face asymmetric warfare** involving raids, ambushes, mines and explosive devices, sabotage etc.

**Arguments against AFSPA**

- **Abuse of power:** It has been alleged that **immunity** granted by the act has led the armed forces to **misuse the powers** and commit offences like enforced disappearances, fake encounters and sexual assault.
  - **Justice Verma committee** (on offenses against women in conflict areas) said AFSPA legitimizes impunity for sexual violence E.g. Kunan Poshpora incident; Thangjam Manorama case in Manipur.
  - Justice **Santosh Hegde Committee** to investigate fake encounters in Manipur described it as a "symbol of oppression".
  - Justice **Jeevan Reddy Committee** recommended removal of absolute immunity under AFSPA.
- **Threat to fundamental rights:** It leads to **suspension of fundamental rights** and liberties guaranteed to the citizens by the constitution. Thus, it weakens democracy.
  - Human rights violations in AFSPA areas are **not inquired into** and followed by adequate action. Thus, it is **against the principle of natural justice**.
- **Diminishing credibility of democracy:** People's disillusionment with democratic setup is **exploited by secessionists** and terror sympathasizers, which leads to more violence & more counter violence creating a vicious cycle.
- **Ineffective:** Critics argue that this act has **failed in its objective** of restoring normalcy in disturbed areas although being in existence for about 50 years.

**Way Forward**

- **Adherence to Human rights:** It needs to be emphasized that **human rights compliance and operational effectiveness are not contrarian requirements**. In fact, adherence to human rights norms and principles strengthens the counter insurgency capability of a force.
- **Robust safeguards:** Protection for the armed forces must be accompanied by provisions that ensure responsibility and accountability, within the parameters of law. It is for this reason that robust safeguards need to be incorporated in the existing or any new law. **Supreme Court's judgement** should be followed in letter and spirit –
  - Every death caused by the armed forces in a disturbed area, be it of a common person or a criminal, should be thoroughly enquired into
  - Even if enquiry finds the victim an enemy, a probe should look into whether excessive or retaliatory force was used.
  - No concept of absolute immunity for an Army personnel who commits a crime.
- **Removing ambiguity in law:** The terms like "disturbed", "dangerous" and "land forces" need to be clearly defined to ensure greater clarity.
- **Ensuring transparency:** Greater transparency in communicating the status of existing cases to include its display on the army and government's web sites.
  - Proactive feedback to petitioners on action taken by the government in past human rights cases.

# 5. MONEY-LAUNDERING

## 5.1. PREVENTION OF MONEY LAUNDERING ACT (PMLA)

**Why in News?**

Recently, Government made the **Prevention of Money Laundering Act, 2002** law stricter via a recent amendment made to the Act through the Finance Act of 2019.

**New amendment**

- The **definition of "proceeds of crime" has been widened** which now includes properties and assets created through any criminal activity even if it is not under the Prevention of Money Laundering Act (PMLA) and it will now be **considered as "relatable offence"**.
- Other amendments have also been brought in **to remove the grey areas and ambiguity in PMLA Act.**

**About Money laundering**

- According to INTERPOL, Money laundering is **concealing or disguising the identity of illegally obtained proceeds** so that they appear to have originated from legitimate sources.
- It is frequently **a component of other, much more serious, crimes such as drug trafficking, robbery or extortion**.
- Some of the common methods of money laundering are **Bulk Cash Smuggling, Shell companies and trusts, Round-tripping, Hawala, False invoicing etc**.
- The advent of cryptocurrency, such as bitcoins, has exacerbated this phenomenon.

**Impact of Money Laundering**

- **Damage to reputation of financial institutions and market:**
  - Weakens the "democratic institutions" of the society
- **Criminal activities:** Provides opportunity to criminals to hijack the process of privatisation
- **Economic Impact:**
  - Destabilises economy of the country causing financial crisis
  - Policy distortion occurs because of measurement error and misallocation of resources
  - Discourages foreign investors
  - Encourages tax evasion culture
  - Results in exchange and interest rates volatility

**About Prevention of Money Laundering Act (PMLA) 2002 Act**

- **Objective**
  - To prevent and control money laundering
  - To confiscate and seize the property obtained from the laundered money; and
  - To deal with any other issue connected with money laundering in India.
- **Defines offence of money laundering**
- **Expanded the reach of the Act by adding many more crimes under various legislations**: It identifies certain offences under the IPC, the Narcotic Drugs and Psychotropic Substances Act, the Arms Act, the Wild Life (Protection) Act, the Immoral Traffic (Prevention) Act and the Prevention of Corruption Act, the proceeds of which would be covered under this Act.
- **Tackles Cross border money Laundering:** It allows Central Government to enter into an agreement with Government of any country outside India for enforcing the provisions of the PMLA, exchange of information for the prevention of any offence under PMLA.
- **Special Courts:** They have been set-up in a number of States / UTs by the Central Government to conduct the trial of the offences of money laundering.
- **Prescribes obligation of banking companies, financial institutions and intermediaries**

**Framework for prevention of money laundering**

- **Institutional framework:** It involves mainly two bodies:
  - **Enforcement Directorate** for investigation and prosecution of cases under the PML.
  - **Financial Intelligence Unit – India (FIU- IND)** for receiving, processing, analysing and disseminating information relating to suspect financial transactions as well as for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies against money laundering.
- **International coordination:**
  - **Financial Action Task Force (FATF):** It is an inter-governmental body established with the objective to set standards and promote effective implementation of legal, regulatory and operational measures to combat money laundering and terrorist financing and other related threats to the integrity of the international financial system.

- **Asia Pacific group:** It works with countries in the Asia-Pacific to generate wide regional commitment to implement anti-money laundering policies and initiatives and secure agreement to establish a more permanent regional anti-money laundering body.
- **Basel Committee on Banking Regulations and Supervisory Practices** issued a statement of principles which aims at encouraging the banking sector to adopt common position in order to ensure that banks are not used to hide or launder funds acquired through criminal activities**.**
- India is also signatory to the **International Convention for Suppression of Financing of Terrorism (1999); the United Nation Convention against Transnational Organised Crime (2000); and United Nation Convention against Corruption (2003).**

**Challenges in tackling money laundering**

- **Predicate-offence-oriented law:** This means a case under the Act depends on the fate of cases pursued by primary agencies only such as the CBI, the Income Tax Department or the police. (Predicate offence- any offence that is component of more serious offence).
- **Growth of Technology**: The enforcement agencies are not able to match up with the speed of growing technologies which makes processes such as placement, layering and integration even more complicated.
- **Non-fulfilment of the purpose of KYC Norms**: KYC norms does not cease or abstain from the problem of **Hawala transactions** as RBI cannot regulate them. Further, such norms are only a mockery as the implementing agencies are indifferent to it. Also, the increasing competition in the market is forcing the Banks to lower their guards and thus facilitating the money launderers to make illicit use of it in furtherance of their crime.
- **Widespread act of smuggling**: there are a number of black market channels in India for the purpose of selling goods offering many imported consumers goods such as food items, electronics etc. which are routinely sold.

**Hawala and Money Laundering**

The word "Hawala" means trust. Hawala is a system of transferring money and property in a parallel arrangement avoiding the traditional banking system.

**How it works?**

In a hawala transaction, no physical movement of cash is there. Hawala system works with a network of operators called Hawaldars or Hawala Dealers. A person willing to transfer money, contacts a Hawala operator at the source location who takes money from that person. The Hawala operator then calls upon his counterpart at the destination location who gives the cash to the person to whom the transfer has to be made, thus completing the transaction.

**Status of Hawala in India**

- Hawala is illegal in India, as it is seen to be a form of money laundering.
- As hawala transactions are not routed through banks, the government agencies and the RBI cannot regulate them.
- In India, FEMA (Foreign Exchange Management Act) 2000 and PMLA (Prevention of Money Laundering Act) 2002 are the two major legislations which make such transactions illegal.

Hawala network is being used extensively across the globe to **circulate black money and to provide funds for terrorism**, drug trafficking and other illegal activities.

- **Lack of comprehensive enforcement agencies**: Separate wings of law enforcement agencies dealing with money laundering, cyber crimes, terrorist crimes, economic offences etc lack convergence among themselves.
- **Tax Heaven Countries**: They have long been associated with money laundering because their financial secrecy laws allow the creation of anonymous accounts while prohibiting the disclosure of financial information.

**Way forward**

- **Enlist common predicate offences**: to solve the problem internationally particularly keeping in mind the trans-national character of the offence of money laundering
- **Awareness and education:** To infuse a sense of watchfulness towards the instances of money laundering which would also help in better law enforcement as it would be subject to public examination
- **Proper Coordination between different stakeholders:** for instance between centre and States**.** Also, there is a requirement to have a **convergence of different enforcement agencies, sharing of information is necessary.**
- **Special cell dealing with money laundering activities:** It should be created on the lines of Economic Intelligence Council (EIC) exclusively dealing with research and development of AML. This Special Cell

should have link with INTERPOL and other international organizations dealing with AML. All key stakeholders, like, RBI, SEBI etc. should be a part of this.

- **Laws in line with conventions:** Countries should criminalise money laundering on the basis of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention).

## 5.2. REPORT ON BLACK MONEY

**Why in news?**

Recently, the Standing Committee on Finance has submitted a report titled, '**Status of Unaccounted Income/Wealth Both Inside and Outside The Country - A Critical Analysis**'.

**Background**

- Although there is **no uniform definition of unaccounted income or black money**, but on a general basis it can be said it is the income from those economic activities that circumvent or otherwise avoid government regulation and taxation.
- It includes all illegal economic activities as well as the income from legal economic activities where the tax is evaded.
- According to the Standing Committee's report, the **sectors that see the highest incidence of black money include** real estate, mining, pharmaceuticals, pan masala, the gutkha and tobacco industry, bullion and commodity markets, the film industry, and educational institutes and professionals.
- The report also notes that it is **difficult to measure black money.**
    - There are neither reliable estimates of black money generation or accumulation, nor is there an accurate well-accepted methodology to make such an estimation.
    - The estimates of the black money in the system provided by the Standing Committee **vary from 7% of GDP to 120% of GDP**, highlighting the wide variance in the methods of estimation.

**Need for the Estimation of Unaccounted/Black Income**

- The unaccounted economy reduces the **size of potential state revenue**.
- To **formulate effective monetary, labor and fiscal policy**, it is crucial to know the level of precision in the estimates of key statistics of the economy, such as, output, price-level and unemployment. Thus, it is crucial to supplement official national accounts statistics with estimates of unaccounted economic activity.
- Some unaccounted economy activities, i.e., **illicit trade in narcotics and arms trading**, are hurtful not only for economy, but also **hazardous for society.**
- It can further lead to
    - a vicious circle of an increase in the budget deficits or tax rates,
    - additional growth of the shadow economy,
    - impact **social welfare in general.**

**Steps taken to tackle the menace of Unaccounted/Black Income**

**Legislative mechanisms**

- Enactment of Central & various state Good & Service Taxes Act
- Enactment of the Black Money (Undisclosed Foreign Income and assets) and Imposition of Tax Act, 2015
- Comprehensive amendment of the Prohibition of Benami Property Transactions Act, 1988
- Fugitive Economic Offenders Act, 2018
- Section 10(38) of the Income Tax Act has been amended to prevent the misuse of exemption by certain persons for declaring their unaccounted income as exempt long term capital gains by entering into sham transactions
- In order to check creation of shell companies which are incorporated outside but controlled from India, the concept of **'Place of Effective Management' (POEM)** for determination of residence of a company incorporated in a foreign jurisdiction, has been introduced in the Finance Act,2016

**Administrative mechanisms and Systems improvement**

- Expanding the ambit of TDS (tax deducted at source) provisions to track more transaction.
- General Anti Avoidance Rules (GAAR) have been implemented with a view to tacking aggressive tax planning with the use of complicated structures

- Various measures taken to reduce cash transactions.

**International Cooperative mechanisms**

- With a view to facilitate and enhance exchange of information under the Tax Treaties, India is pro-actively engaging with the foreign Governments and has signed Tax Treaty framework with 146 foreign jurisdictions. E.g. Foreign Account Tax Compliance Act with the US.
- The Government of India has also joined the Multilateral Competent Authority Agreement (MCAA) for Automatic Exchange of Information as per Common Reporting Standards (CRS).
- India has amended its Double Taxation Avoidance Agreements with Mauritius, Singapore and Cyprus to enable measures concerning prevention of tax evasion and tax avoidance.

**Judicial Efforts**

On the directions of the Supreme Court, the government in 2014 constituted the Special Investigation Team (SIT) on black money. The SIT has so far submitted seven reports to Hon'ble Supreme Court.

**Way Forward**

Apart from all these measures, the **standard of morality** must be increased in the public domain. Here the role of, political and bureaucratic leadership along with other prominent players from private sector and civil society, is crucial.

# 6. MILITARY MODERNISATION

## 6.1. DEFENCE PROCUREMENT IN INDIA

**Introduction**

- India is **one of the largest importers of conventional defence equipments** and spends about 31.1% of its total defence budget on capital acquisitions.
- About 70% of its defence requirements are met through imports.
- However, defence procurement in India is marred with following issues:
  - **Monopoly of the public sector** and limited experience of private sector in defence manufacturing
  - **Lack of well thought out strategic plans** with foreign countries that often impedes technology transfers.
  - **Lack of an institutional mechanism** that can lay out a long-term roadmap for the defence industry.
  - **Limited capability to absorb/assimilate technology.**
  - **Limited R&D base and lack of adequate skilled manpower**

**Potential of Defence Manufacturing in India**

- **Achieving strategic independence**- so as to give India the necessary operational preparedness and reduce dependence on foreign nations.
- **Cost effective defence equipment**- could be obtained by the forces, rather than spending crucial FOREX on foreign procurements.
- **Generation of employment**- Indian policy seeks to a turnover of Rs.1.7 trillion in defence sector by 2025, with an additional investment of Rs. 70,000 crore, creating two-three million jobs.
- **Defence exports**- The government has earn resources to the tune of Rs. 35,000 crore. Also it can add to India's soft power and negotiating ability with other countries.

**Initiatives to improve Defence manufacturing in India.**

- Government is establishing **two Defence Industrial Corridors** (Uttar Pradesh and Tamil Nadu).
- Launch of **'Mission Raksha Gyan Shakti'** which aims to provide boost to the IPR culture in indigenous defence industry.
- **Defence Investor Cell** has been created in the Ministry to provide all necessary information required for investment in the sector.
- Innovations for **Defence Excellence (iDEX)** has been launched for engaging Industries Individual Innovators, R&D institutes and Academia.
- Government has notified **Policy for indigenisation of components and spares** used in defence platforms. It seeks to create an industry ecosystem which is able to indigenize the imported components for defence equipment.
- **FDI Policy** has been revised to allow under automatic route upto 49% and beyond 49% through Government route.
- A **Technology Development Fund (TDF)** has been setup to encourage participation of public/private industries especially MSMEs, through provision of grants.
- Steps are being taken to discontinue the preferential treatment given to Defence Public Sector Undertakings (DPSUs) to create a level playing field.

**Defence Procurement Procedure (DPP)-2016**

- DPP is to ensure timely procurement of military equipment, systems and platforms as required by the Armed Forces in terms of performance capabilities and quality standards, through optimum utilisation of allocated budgetary resources.
- **Defence Procurement Procedure (DPP)-2016** focuses on **institutionalising, streamlining and simplifying defence procurement procedure** to give a boost to "Make in India" initiative, by promoting indigenous design, development and manufacturing of defence equipment, platforms, systems and sub-systems.
- Capital Acquisition schemes under DPP are broadly classified as
  - **Buy:** Under it procurements are categorised as: **Buy {Indian-IDDM (Indigenously Designed, Developed and Manufactured)} , Buy (Indian) and Buy (Global).** The three categories under it refer to an outright purchase of equipment.
    - ✓ The category of **Buy (Indian - IDDM)** has been accorded top most priority for procurement of capital equipment.
  - **Buy and Make:** Under it the procurements are categorised as **Buy and Make (Indian)** and **Buy and Make.** It involves an initial procurement of equipment followed by indigenous production through comprehensive Transfer of Technology.
  - **Make:** It aims at developing long-term indigenous defence capabilities.
    - ✓ The 'Make' Procedure has been simplified with provisions for funding of 90 % of development cost by the government to Indian industry and **reserving projects not exceeding development cost of Rs. 10 crore (government funded) and Rs. 3 crore (industry funded) for MSMEs.**

- DPP also provides for a **Defence Offset Policy** which seeks to leverage the capital acquisitions to develop Indian defence industry by fostering development of internationally competitive enterprises; augmenting capacity for research and development in defence sector and to encourage development of synergistic sector like civil aerospace and internal security.
    - The offset can be discharged by many means such as direct purchase of eligible products/services, FDI in joint ventures and investment towards equipment and transfer of technology.

**Role of Private sector in Defence procurement**

- **Effective use of defence budget:** At present, major part of the defence budget is spent in importing foreign equipments with **no transfer of technology**. With increased participation of Private sector indigenous capacity building and durable asset creation will be the benefits which would reduce import dependence.
- **Growth in economy:** Defence, being a major manufacturing sector, acts as a multiplier in the economy, which would lead to entrepreneurship, investment and employment.
- **Procurement will be streamlined:** dependence on foreign players causes delay in procurements and at times substandard quality is provided by them, there are issues regarding getting the spare parts too.
- **Strategic Autonomy & self-reliance:** this becomes very important in critical situations like war. During Kargil war, US had withdrawn its GPS support which had a severe impact on casualty.

**Measures to improve defence procurement**

- Need to do **competency mapping** of the private sector and nurture their growth accordingly.
- **Development of capabilities** of micro, small and medium enterprises, especially with regard to manufacture of defence spare parts and equipments.
- **Improved Procurement-**
    - Faster **procurement cycles**, self-certification to save time and synchronise procurement cycles with technological cycles.
    - Introduction of an **end-to-end digitised procurement system** with accountability and timelines strictly defined
    - **Time-bound production targets** must be supported by timely procurement with budgetary support.
- **India's strong IT industry** needs to be leveraged for the defence sector, especially in regards to developing new technologies.
- Focus has to be on **achieving state of the art technologies**, rather than mere self-reliance, which yield sub-standard indigenous products.
- **Rules need to be more transparent** so that decision making and consistency in public policy is maintained to avoid scams like Rafale Deal.

## 6.1.1. STRATEGIC PARTNERSHIP POLICY

**Why in News?**

The Governments of India has started acquisition of defence infrastructure under the newly adopted **Strategic Partnership Policy**.

**About Strategic Partnership Policy**

- Under this policy an **Indian private company** would be selected in each segment which would tie up with shortlisted **global Original Equipment Manufacturer (OEM)** to manufacture the platforms in India under technology transfer. This will promote **Indian private sector participation** in defence manufacturing.
- It was first suggested in 2015 by **Dhirendra Singh Committee** and was introduced by **Defence Procurement Procedure 2016.**
- These few Indian private companies will be designated as **Strategic Partners (SP)** that would assume the role of system integrators and also lay a strong defence industrial foundation. The Government will co-opt them for 'Buy and Make' and Government-to-Government procurement programmes.
- A **49 per cent FDI cap** has been kept for setting up ventures under this for the production of defence platforms and the companies have to be in control of Indian entities.
- Government has started acquisition of defence equipments under **Strategic Partnership Policy,** such as **111 Naval Utility Helicopters (NUH) and 6 P-75 (I) submarines**

**Significance of SPP**

- It will **boost self-reliance** by encouraging indigenous defence industry and aligning the defence sector with the 'Make in India' initiative leading to reduction in dependence on imports.
- Help **enhance competition, increase efficiencies**, facilitate faster and more significant absorption of technology

- **Create a tiered industrial ecosystem**, ensure development of a wider skill base, trigger innovation and enable participation in global value chains as well as promote exports.
- Can **bridge the long-standing trust gap** between the Indian private sector and Ministry of Defence.
- **Streamlining procurement** as dependence on foreign players causes delay in procurements and at times substandard quality is provided by them, there are issues regarding getting the spare parts too.

## 6.2. WOMEN IN COMBAT ROLE

**Why in News?**

Recently Government has taken a decision to induct women for the **first time ever in Personnel Below Officer Rank (PBOR) in corps of Military Police** in a graded manner to eventually comprise 20 per cent of total Corps.

**Women Representation in Armed Forces**

- Currently the Army has **3.80 per cent of its workforce as women, the Air Force has 13.09 per cent and the Navy 6 per cent.**
- Currently, women are allowed in select areas such as medical, legal, educational, signals and engineering wings of the Army.
- The **Indian Air Force** is the **only armed force in India to put women in combat roles**. It has inducted about five women fighter jet pilots, all of whom are presently at various levels of training.
- Recently, the Ministry of Defence has decided to **induct women as sailors** in the Indian Navy.

**Arguments in favor of Women in Combat role**

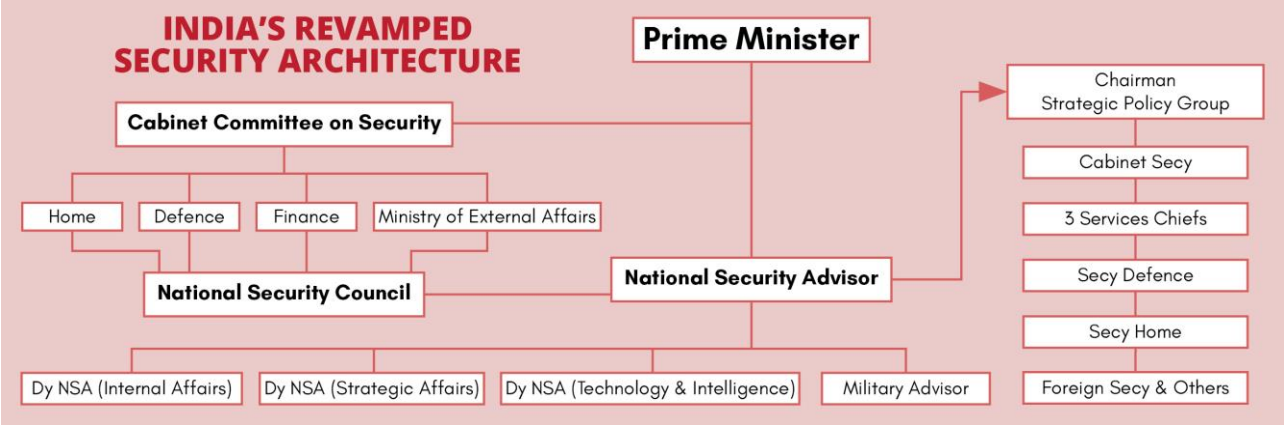
- **Increasing gender Representation:** It would be a radical move to gender parity in one of the world's most-male dominated professions. This is the trend globally as well.
- **Military Readiness:** Allowing a mixed gender force keeps the military strong. The all-volunteer forces are severely troubled by falling retention and recruitment rates. Widening the applicant pool for all jobs guarantees more willing recruits.
- **Effectiveness:** The blanket restriction for women limits the ability of commanders in theater to pick the most capable person for the job.
- **Tradition:** Training will be required to facilitate the integration of women into combat units. Cultures change over time and the masculine subculture can evolve too. Many previously masculine professions have been successfully opened to women over the past century.
- **Cultural Differences & Demographics:** Allowing women to serve doubles the talent pool for delicate and sensitive jobs that require interpersonal skills not every soldier has. Having a wider personnel base allows militaries to have the best and most diplomatic soldiers working to end conflict quickly.
- **Career advancement:** As combat duty is usually regarded as necessary for promotion to senior officer positions, denying female personnel this experience ensures that very few will ever reach the highest reaches of the military.
- **Technology advancement**: Landscape of modern warfare has changed with more sophisticated weapons, greater focus on intelligence gathering and emergence of cyberspace as arena of combat. Brute force, often a reason for non-inclusion of women, is less necessary today.

**Arguments against Women in Combat Role**

- **Condition in Army:** The field conditions in the Army are much more rugged and proximity to comrades and adversary poses greater challenges.
- **Physical Ability:** Traditionally women are seen physically not suited for certain jobs. The standards of physical fitness have been set to suit men, and women attempting to reach them will over-stretch themselves.
- **Military readiness:** Certain situations such as pregnancy can affect the deployability of a unit when the unit has a disproportionate number of women or is understaffed.
- **Tradition**: Men, especially those likely to enlist, maintain traditional gender roles. Harassment and resentment of the presence of women in a military subculture can likely become a problem.
- **Abuse by Enemy**: Both male and female prisoners are at risk of torture and rape, which raises question regarding **safety and dignity** of women.

All matters concerning the security of the country have to be considered in a **dispassionate manner**. The whole concept of women's induction in the services, therefore, has to be viewed in a **holistic and objective manner** and not as a question of conquering the so-called 'last male bastion'. Therefore, there should be a **gradual integration of women in the services** along with continuous and **periodical performance auditing** of both male and female soldiers. The army of the future could be all the stronger for being all inclusive.

## 6.3. NATIONAL SECURITY ARCHITECTURE IN INDIA




**Functions of different organizations**

- **Cabinet Committee on Security (CCS)**
  - It is the apex body for **executive action on matters of national security.**
  - CCS is responsible for **Political oversight and decision making on national security** ensuring the democratic principle of civilian and political control of the apparatus.
  - Both National Security Council and CCS have a common membership which **helps in easier decision making and implementation**.
- **Strategic Policy Group (SPG).**
  - It is mandated **to publish National Defense Review- a draft of short term and long-term security threats and defense matters for consideration of NSC**.
  - The SPG shall be the **principal mechanism for inter-ministerial coordination and integration of relevant inputs in the formulation of national security policies.**
  - The Cabinet Secretary will coordinate the implementation of SPG decisions by the Union Ministries and departments and State governments.
- **Defence Planning Committee**
  - It is tasked **to recommend policy measures** to improve India's defence capability and preparedness, and national security in general.
  - To assist in the **creation of national security strategy**, international defence engagement strategy, roadmap to build a defence manufacturing ecosystem, strategy to boost defence exports, and priority capability development plans.

**Recent Reforms in National Security Architecture**

- **Three deputy National Security Advisors** have been appointed instead of just one, while the post of military advisor has been revived.
- **A Defence Planning Committee**, headed by the NSA, has been set up to align National security needs and defense resources into one decision making box.
- **National Security Advisory Board** has been revived with major appointments in recent months.
- The Strategic Policy Group (SPG) formed to assist the National Security Council (NSC) has been reconstituted with National Security Advisor Ajit Doval as its chief.

**Issues in the structure**

- **No national security/defence vision:** Ideally, the country should have an overall national security document from which the various agencies and the arms of the armed forces draw their mandate and create their own respective and joint doctrines which would then translate into operational doctrines for tactical engagement.
- **No regular meetings:** Given that the NSC and the Cabinet Committee on Security have exactly the same membership, the former rarely meets which weakens the national security system of the country.

- **No legal power and accountability to parliament:** NSA has no legal powers as per the government's allocation of business rules and it is not accountable to Parliament.
- **Lack of coordination**: There is **little conversation between the armed forces and the political class**, and even lesser conversation among the various arms of the forces.
- **Politicization of the actions of the armed forces.**

**Way forward**

- **More accountability and legal formality:** The job of the National Security Adviser needs to be reimagined by making him accountable to the parliament.
  - The K.C. Pant Task Force in the late 1990s had recommended the creation of an NSA with the rank of a Cabinet Minister.
- **More powers to NSC**: If the NSC is to be made more useful, the government's allocation of business rules should be amended to give more powers to the NSC and its subordinate organisations, such as the Strategic Policy Group.
- **Increasing professionalism:** Professionalizing the IAS and IDAS cadre and creating a specialized national security cadre with requisite technical expertise.
- **Creation of a coordinating center:** For effective operationalisation of terror related intelligence inputs that was sought to be earlier addressed by setting up a National Counter-Terrorism Centre (NCTC).
- **Manpower policy:** There is need for the manpower policy of the Government for intelligence and security agencies to attract the best talent and to retain them.
- **Comprehensive National Security Strategy:** There is also an urgent need for India to evolve a bipartisan policy on security-governance by developing a Comprehensive National Security Strategy.

## 6.3.1. PERMANENT CHAIRMAN OF THE CHIEFS OF STAFF COMMITTEE

**Why in News?**

The three services have agreed on the appointment of a Permanent Chairman of the Chiefs of Staff Committee (PCCoSC).

**Current Structure in India**

- The Chief of Staff Committee (CoSC) consists of Army, Navy and Air Force chiefs.
- It is headed by the **senior-most** of the three chiefs **in rotation** till the he retires.
- It is a platform where the three service chiefs discuss important military issues.
- It advises the Defence Minister and through him all the matters relating to military are seen further by Cabinet Committee on Political Affairs.

**About PCCoSC**

- It is proposed to be headed by a **four-star military officer**, who will be equivalent to chiefs of army, airforce and navy.
- He would **look into joint issues of the services** like training of troops, acquisition of weapon systems and joint operations of the services.
- He would also be **in-charge of the tri-services command** at Andaman and Nicobar Islands.
- The post has also been referred to as **Chief of Defence Staff.**
- He will **head the Chiefs of Staff Committee meetings**.
- Various committees such as the **Kargil Review committee** led by K Subramaniam and the **Naresh Chandra committee** of 2011 recommended a permanent chairman.

**Arguments in favour of PCCoSC**

- **Better Coordination:** It will improve jointness in military command by integration in projects and resource sharing. For example during 1962 and 1965, all three segments of the armed forces face difficulties in coordination.
- **Unfragmented advice:** The PCCoSC is envisaged as a single-point military adviser to the government.
- **Better defence acquisition:** It would also improve capacity of the armed forces on defence acquisition by removing time and cost overruns.
- **Quick Decision-making during War:** Often during war a difficult decision can only be made by a specially selected defence chief and not by a committee like the CoSC that operates on the principle of the least common denominator.

**Challenges to setting up PCCoSC**

- **Threat to Democratic Process:** It is apprehended that the Defence Services will become too powerful and subvert civilian control over the military with possibilities of a military coup.
- **Status Quo:** The present arrangement of Chief of Staff Committee (CoSC) has served us well over the years and hence there is resistance against "unnecessary change".
- **Resistance within the armed forces:**
  - There is said to be inhibition amongst Service Chiefs over the years that their position would get undermined if the CDS were to be appointed.
  - The feeling among the smaller Services, particularly the Air Force, of Army dominance in defence policy formulation. Some fear that a CDS may lead to a situation like the one that prevailed before 1947, when the Army was the dominant Service.
- **Resistance within Bureaucracy:** There is said to opposition by the civilian bureaucracy as their control over the higher defence set up would be diminished.
- **Ceremonial Post:** There is also a concern that the post may become a ceremonial post without any clear cut roles and responsibilities.

## 6.4. CENTRAL ARMED POLICE FORCES

**Why in News?**

Recently, Standing Committee on Home Affairs (Chairperson: Mr. P. Chidambaram) submitted its report on **Working Conditions in Central Armed Police Forces.**

| **Central Armed Police Forces under Administrative Control of Ministry of Home Affairs** | |
|---|---|
| **Border Guarding Forces** | **Non-Border Guarding** |
| **Assam Rifles:** Guards the Indo-Myanmar border. | **Central Industrial Security Force (CISF):** Provides security for key installations. |
| **Border Security Force (BSF):** Guards the Indo-Pakistan and Indo-Bangladesh borders. | **Central Reserve Police Force (CRPF):** Deployed for maintaining internal security. |
| **Indo-Tibetan Border Police (ITBP):** Guards the Indo-China border. | **National Security Guard (NSG):** Deployed for anti-terrorist activities. |
| **Sashastra Seema Bal (SSB):** Guards the Indo-Bhutan and Indo-Nepal borders. | |

**Issues identified by the Report**

- **Bureaucratisation of Armed Forces**: Majority of the higher posts of the top hierarchy are filled by deputations (IPS officers), who most of the times failed to take adequate steps for the welfare of the cadre officers.
- **Higher Vacancies and lack of promotional prospects:** There is an acute stagnation in the all cadre of CAPFs, which in turn is affecting the morale and efficiency of forces and reflect lack of foresight, planning, and proactive estimation of future vacancies.
- **Absence of a robust in-house grievance redressal mechanism**, which prompted a Soldier from BSF in 2017 to use Social Media to raise his concerns.
- **Ineffective Coordination Between State Police and The CAPF Leadership**: States are over-dependent on the CRPF for maintaining various law and order situations. The continuous deployment of training companies affects the operational efficiency of the CRPF, as well as denies them training and rest.
- **Poor Infrastructure: Lack of electricity** at several installations of **Border Out Posts (BOPs),** seriously affects the working conditions of the personnel as well as operations of the CAPFs.
  - An inquiry on a 2010 incident in Dantewada, found that the force's camp lacked basic facilities, had minimal security and deplorable living conditions.
  - These affect the overall moral of the forces leaving them psychologically vulnerable. Often incidences of suicides and shooting down of the colleagues come in the light.
- **Road connectivity and mobility:** There is a delay in execution of road projects which affect mobility of personnel. This happens due to delay in obtaining forest/wildlife clearances, hard rock stretches, limited working season, difficulties in availability of construction materials, etc.
- **Shortages of Arms and Ammunition**: There are inordinate delays in procurement of combat-ready equipment and inadequate medical facilities, especially when personnel are deployed in hostile environment.

**Recommendations**

- **Ending IPS hegemony**: The nature of duty of CAPF is more similar to that of the Armed Forces and it would make more sense to bring more officers from the Armed Forces on deputation.
    - However, MHA has contested the same by justifying that the presence of IPS officers in every CAPF increases inter-departmental coordination between various CAPFS and State and therefore IPS officers are best suited to lead and provide supervisory directions to any CAPFs in an effective, efficient and impartial manner.
- **Modernization of the Force** must be given utmost priority as this Force not only has to face any enemy from across the border but also vagaries of nature.
- **Issue specific Counter Plan rather than One-Size Fits All Approach:**
    - **For J&K:** MHA should adopt a multi-pronged strategy that prevents youth from joining militancy, curbs their financing, and simultaneously launch counter-insurgency operations.
    - **For Left Wing Area:** MHA should make efforts to procure mine-resistant vehicles. This could be done through import or domestic manufacturing under the 'Make in India' programme.
- **Expedite Cadre Review** of these forces as it's is essential to maintain their organizational structure and ensures completion of project in a time-bound manner.
- **Setting up Dedicated Research And Development (R&D) Wing:** It recommended that due to the unique issues faced by the CRPF, such as large size and areas of deployment, creation of a dedicated R&D unit of its own should be explored, to deal with issues peculiar to the CRPF such as Improvised Explosive Devices (IEDs), and bullet proofing of vehicles.

# 7. MISCELLANEOUS

## 7.1. CLIMATE CHANGE- A SECURITY ISSUE?

**Why in news?**

Recently India raised its concerns at the sheer urgency shown by nations at the UN to **declare climate change a global security issue.**

**Background**

> **Article 39 of UN charter**
> The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken to maintain or restore international peace and security.

- Many Scholars declared Climate Change as **Warming War** which requires intervention of United Nation Security Council as per its mandate under **article 39 of UN charter**.
- **The Warming War is a metaphor** (like Cold War) which conveys how climate change acts as a driver of such conflict, as its impacts accumulate and multiply to threaten the security of human life on earth.

**Why Climate Change is a security issue?**

- **Earth's limited resources** are under pressure as demand for food, water, and energy is increasing. Widespread unemployment, rapid urbanization, and environmental degradation can cause persistent inequality, political marginalization, and unresponsive governments leading to instability and conflict.
- In above context **United Nation Environment Program has identified seven factors** where climate change acts as threat multiplier to security and peace of states and society.
  - **Local resource competition:** As pressure on local resources is increasing, competition can lead to instability and even violent conflict in absence for proper dispute resolution.
  - **Livelihood insecurity and Migration**
    - ✓ Climate change will **increase the insecurity of farmers** who depend on natural resources for livelihood. It could push them to migrate and turn to informal and illegal source of income.
    - ✓ **As per World Bank estimates by 2050**, about 140 million people will be forced to leave their place of origin in South Asia, Africa and Latin America.
  - **Extreme weather events and disasters:** Disasters will exacerbate fragile situation and can increase people vulnerabilities especially in countries affected by conflict.
  - **Volatile food price**
    - ✓ Climate change is likely to disrupt food production in many regions, increase prices, market volatility and heightening risk of protest, rioting and civil conflicts.
    - ✓ As per IPCC assessment by 2080 there will be 770 million undernourished people by 2080 due to climate change.
  - **Transboundary water management**
    - ✓ It is a frequent source of tension. As demand grows and climate impact affects availability and quality, competition over water use will likely exert pressure at local, regional and global level.
    - ✓ According to recently released Hindukush-Himalayan Assessment report with current emission level two-third of glaciers in the region will be lost by 2100 and cause water crisis for 2 billion people.
  - **Sea level rise and coastal degradation**
    - ✓ Rising sea level will threaten the viability of low lying areas even before they are submerged, leading to social disruption, displacement and migration. Also, disagreement over maritime boundaries and ocean resources may increase.
    - ✓ As per IPCC 5$^{th}$ assessment report sea level rise can be 52-98 cm by 2100.
  - **Unintended effects of climate change:** As the climate adaptation and mitigation policies are more broadly implemented, the risks of unintended negative effects-particularly in fragile regions will also increase. In countries with poor institutional capacity and governance, this may lead to **immense political pressure and ultimately civil war**.

**Reason for support of UNSC intervention**

- If the UNSC declares the impacts of climate change an international threat then **military and non-military sanctions** could be invoked**.**

- The sanctions would be available to the council in the event of states not meeting their Paris Agreement obligations. **Economic sanctions** could also be placed upon corporations that currently operate with relatively little international scrutiny.
- Supporters of such declaration cites slow and ineffective progress of climate negotiations (under UNFCCC) and demand a rapid response to decreasing GHG emissions **to stop temperature rise below 2°C.** It'll bring element of **coercion** in climate agreements.
- These measures could include the **deployment of peacekeeping forces and increased humanitarian assistance** surrounding direct and indirect climate induced crises.

**Why India is opposing?**

- **Expansion of Jurisdiction:** India opposes the redefining of Charter by Security Council and expansion of its jurisdiction when it has **failed to fulfill even its original mandate.**
- **Exclusive nature of UNSC:** Climate Justice can be ensured by an **inclusive institution like UNFCCC,** which is missing in an exclusionary and opaque body of UNSC.
- **Complex nature of problem:** Climate Change is a multidimensional issue involving not just political but social, economic, demographic and humanitarian factors. UNSC has mainly a political mandate and narrow view of looking at a problem.
- **Past record of UNSC:** Historically the conduct of UNSC has remained biased towards the member countries own geo-political interests. It has adopted a selective approach and lack uniformity in its decisions. Climate justice which demand a fair and bipartisanship approach (e.g. Principle of Common But Differentiated Responsibility) can be jeopardized under the ambit of UNSC.
- It also **undermines the sovereignty of countries** and right to self-determination.

## 7.2. WEAPONIZATION OF SPACE

**Why in News?**

Recently, US proposed to create a new US "Space Force," which raises the debate on Weaponization of Space.

**About Weaponization of Space**

- It includes **placing weapons in outer space or on heavenly bodies** as well as **creating weapons that will transit outer space** or simply travel from Earth to attack or destroy targets in space.
  - **Examples:** include the placing of orbital or suborbital satellites with the intention of attacking enemy satellites, using ground-based direct ascent missiles to attack space assets, jamming signals sent from enemy satellites, satellite attacks on Earth targets etc.
- The weaponization of space is **different from the militarization of space,** which includes using space-based assets for C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance).
  - The militarization of space assists armies on the conventional battlefield, whereas via the weaponization of space, **outer space** itself emerges as the battleground, sometimes referred to as the **"fourth frontier of war."**
- Development projects for militarisation and weaponisation of outer space have been on the increase with the aim of one country **achieving military dominance over the other in outer space.**

**Outer Space Treaty**

- The Outer Space Treaty, formally the Treaty on **Principles Governing the Activities of States in the Exploration and Use of Outer Space,** including the Moon and Other Celestial Bodies, is a treaty that forms the basis of international space law.
- It was adopted by the UN General Assembly in 1963 and entered into force in 1967.
- **India** is a signatory to this treaty, and ratified it in 1982. The Outer Space Treaty prohibits only weapons of mass destruction in outer space, not ordinary weapons.
- It mandates that use of outer space shall be carried out for the benefit and in the interests of all countries and shall be the province of all mankind.

**Prevention of an Arms Race in Outer Space** (PAROS)

- It is a UN resolution that reaffirms the fundamental principles of the 1967 Outer Space Treaty and advocates for a **ban on the weaponization of space**.
- It is currently being discussed in the **Conference on Disarmament** (CD).
- Till now, the parties have discussed various issues and possible solutions. Some parties like the Russian federation and Venezuela, have even pledged to **not be the first to deploy** any type of weapon in outer space.
- It would prevent any nation from gaining a military advantage in outer space.

**Implications of Space weaponisation**

- **Opening up of a new front**: As powerful countries will start weaponizing the space, other countries will also jump into this race, hence disrupting global balance of power .
  - The ensuing arms race for weaponisation of outer space could also create an environment of uncertainty, suspicion, competition and aggressive deployment between nations, which may lead to war.
- **Damaging other projects in space:** It would put at risk the entire range of commercial satellites as well as those involved in scientific explorations.
- **Space debris issues**: The mid-course missile defence, which shatters missiles in outer space, poses enormous dangers because it would create a massive amount of debris. Also the increase in interceptors will result in colliding with each other.
- **Occupying radio frequencies and orbital slots**: As the peaceful scientific and commercial operations in space increase yearly, so does their reliance on radio frequencies and their need for an orbital path, particularly in the geosynchronous orbit. Some countries may reserve an orbital slot and monopolise the limited number of orbital slots.

**Way forward**

- **Need for Multilateral treaty:** It will be needed to prevent arms race as majority of UN member states are concerned that the weaponisation of outer space.
- **1967 Outer Space Treaty:** The UN is further striving to improve and facilitate the inhibition of an arms race in outer space by strengthening the 1967 Outer Space Treaty through various committees on prevention of an arms race in outer space and resolutions on establishment of transparency and confidence- building measures among the countries.
- **Information sharing:** In order to increase situational awareness of space objects already in space, as well as their purposes, states should submit valid information to international institutions which can then organize the data and provide open-source information to all about the situation in space.
- **Ban the deployment** and testing of weapons in space.

## 7.2.1. MISSION SHAKTI

**Why in news?**

Recently, India tested its **first anti-satellite (ASAT) missile** as part of **'Mission Shakti'** against a previously launched **"live" satellite**.

**Indian Ballistic Missile Defence Programme**

- It is an initiative to develop and deploy a **multi-layered** ballistic missile defence system to **protect India from ballistic missile attacks**.
- It has two broadly defined target tiers, called **endo-atmospheric and exo-atmospheric.**
- Mission Shakti falls in the exo-atmospheric category.

**Background**

- An anti-satellite weapon is anything that destroys or physically damages or incapacitates a satellite for strategic military purposes. Only the **United States, Russia, China, and now India** have demonstrated this capability successfully.
- **Mission Shakti** is India's response to the potent case of future **weaponization of space**, where enemy nation can indulge in **space war to disrupt critical infrastructure** of the nation.
- The DRDO's **Ballistic Missile Defence interceptor** was used, which is part of the ongoing ballistic missile defence programme.

**Need for the mission**

- India's space programme is a **critical backbone** of India's **security, economic and social infrastructure**. The test was done to **verify** that India has the **capability to safeguard our space asset**s.
- The capability achieved through the Anti-Satellite missile test provides **credible deterrence against threats** to our growing space-based assets from long-range missiles, and proliferation in the types and numbers of missiles.

- A-SAT is a sub-set of a **space military strategy**.
  - It would require Space Situational Awareness (SSA), involving ground-based radars, optical telescopes and satellite constellations.
  - The strategy architecture would also require space-based C4ISR (Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance), Anti-Satellite (ASAT) and Ballistic Missile Defence (BMD) capabilities.

**Is India entering into an arms race in the outer space?**

**Launch of first anti-satellite missile** as part of **'Mission Shakti'** by India has put a question on its stance on weaponization of outer space.

- India has **no intention of entering** into an arms race in outer space. India has always maintained that space must be used only for **peaceful purposes**. India is against the **weaponization of Outer Space** and support international efforts to reinforce the safety and security of space based assets.
- India is a party to all the **major international treaties** relating to Outer Space.
- India already implements a number of **Transparency and Confidence Building Measures (TCBMs)** – including
  - Registering space objects with the UN register,
  - Prelaunch notifications,
  - Measures in harmony with the UN Space Mitigation Guidelines,
  - Participation in **Inter Agency Space Debris Coordination** (IADC) activities with regard to space debris management,
  - Undertaking SOPA (**Space Object Proximity Awareness** and COLA (**Collision Avoidance Analysis)** etc
- India also supported **UNGA resolution 69/32** on **No First Placement of Weapons** on Outer Space.
- India supports the substantive consideration of the **issue of Prevention of an Arms Race in Outer Space** (PAROS) in the Conference on Disarmament where it has been on the agenda since 1982.
- India expects to play a role in the future in the **drafting of international law** on prevention of an arms race in outer space including inter alia on the prevention of the placement of weapons in outer space in its capacity as a major space faring nation with proven space technology.

**Significance of Mission Shakti**

- **India's entry in the elite group-** India is only the 4th country to acquire such a specialised and modern capability. The use of ASAT is seen as crossing new frontier just like India's 1998 nuclear tests.
- **Entire effort is indigenous-** by the Indian scientists in the DRDO. It adds to India's credentials, given that for many decades India was kept away from acquiring key technologies, forcing the country to develop its own space and nuclear capabilities.
- **Addressed the concerns of Space Debris-** DRDO has said that all the debris of India's ASAT will **decay** in 45 days.
- **Develops credible deterrence-** The anti-satellite space technology shows India's focus on security challenges, emanating beyond Pakistan. ASATs can be used to intercept and jam communication or military satellites of enemy countries and stop them from communicating with their soldiers.
- **Test done before any kind of international sanctions come in place-** as UN General Assembly is trying to bring about an international legally binding document on the prevention of an arms race in outer space that would include the prevention of placement of weapons in outer space among other thing (PAROS).
- **Did not invite international criticism-** as major countries expressed symbolic concern, without severe criticism. In contrast, the Chinese test in 2007 provoked international ire because it destroyed a satellite. The act violated the principles of the Outer Space Treaty. This is not the case with India.
- **Won't impact other strategic interests-** e.g. it will not have any effect on India's status in the MTCR (Missile Technology Control Regime) or other such treaties.

**Way Forward**

- India's space capabilities do not threaten any country and nor are they directed against anyone. At the same time, the government is committed to ensuring the country's national security interests and is alert to threats from emerging technologies.
- At the same time, world should evolve framework to prevent any space weaponization through the following-
  - A stringent "no space weaponization" policy needs to formulated and adhered to by all countries in order to protect the interest of all.
  - A monitoring system must be established so as to catch violators.
  - Rules must be formulated for satellite based military assistance.
  - The UN Outer Space Treaty only talks about using the space about peaceful. purposes. Issues like militarization and weaponization must be worded out.