



SECURITY

Classroom Study Material 2020

(September 2019 to September 2020)

SECURITY

Table of Contents

1. CYBERSECURITY _____	2	6. POLICE MODERNIZATION _____	31
1.1. 5G and Cybersecurity _____	5	6.1. Police Preparedness During COVID-19 Pandemic _____	32
1.2. Artificial Intelligence and National Security _____	6	7. MILITARY MODERNIZATION _____	35
1.3. Fake News _____	8	7.1. Defence Production _____	35
2. DATA PROTECTION _____	11	7.1.1. Draft Defence Production and Export Promotion Policy (DPEPP) 2020 _____	36
2.1. The Personal Data Protection Bill, 2019 _____	12	7.2. Defence Acquisition Procedure, 2020 _____	36
2.2. Non-Personal Data _____	13	7.3. Permanent Commission and Command positions to Women Army Officers _____	38
2.3. Security issues with Aarogya Setu App _____	14	7.3.1. Women in Combat Role _____	39
3. BORDER SECURITY AND MANAGEMENT _____	16	7.4. Chief of Defence Staff (CDS) _____	40
3.1. Border Infrastructure _____	17	7.5. Theatre Command in India _____	41
3.2. Challenges in Border Areas and recent initiatives to tackle them _____	18	8. EMERGING DIMENSIONS OF WARFARE _____	44
4. EXTREMISM AND TERRORISM _____	20	8.1. Hybrid Warfare _____	44
4.1. Anti-Terror Laws in the Country _____	21	8.2. Space Warfare _____	45
4.1.1. Unlawful Activities (Prevention) Amendment Act, 2019 _____	21	8.3. Directed Energy Weapons (DEWs) _____	47
4.1.2. NIA (Amendment) Act, 2019 _____	22	9. MISCELLANEOUS _____	49
4.2. "Lone Wolf" Attacks _____	23	9.1. Piracy in the Indian Ocean Region _____	49
5. INSURGENCY IN THE NORTHEAST _____	26	9.2. Militarization of Andaman and Nicobar Islands _____	51
5.1. Naga Peace Talks _____	27	9.3. India's Nuclear Doctrine _____	53
5.2. The Bodoland Dispute _____	28	9.4. Epidemics and National Security _____	55
5.3. Bru Refugee Crisis _____	29		

FOUNDATION COURSE 2021 PRELIMS CUM MAINS | GENERAL STUDIES

TURN YOUR ROOM INTO A CLASSROOM

Features of the Program:

- Includes a comprehensive coverage of all topics of GS Mains, GS Prelims, CSAT and Essay
- Comprehensive coverage of Current Affairs through Live / Online classes of PT 365 & Mains 365 & News Today - A Daily Current Affairs Initiative
- One senior mentor will be provided for each group consisting of 25 students for regular mentoring, performance monitoring, guidance and support. It will be done through various modes like Google Hangouts & Groups, email and telephonic communication.

LIVE / ONLINE CLASSES

Regular Batch	25 NOV, 10 AM 27 OCT, 5 PM
Weekend Batch	21 JUNE 9 AM

1. CYBERSECURITY

Introduction

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.

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.

Challenges in ensuring cyber security

- **Widespread digital illiteracy:** which makes Indian citizens highly susceptible to cyber fraud, cyber theft, etc.
- **Use of 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.

Cybersecurity threats from China

- **Chinese mobile apps:** India has the world's highest number of Internet users downloading millions of apps every year. However, 80% of these apps are insecure from security standpoint.
- **Intellectual Property:** According to an American intelligence agency report, Chinese firms have stolen billions of terabytes of data from 141 companies across 20 major industries.
- **Cyber-espionage:** According to an American cybersecurity report, People's Liberation Army's Advanced Persistent Threat (APT) unit that has been accused of several computer hacking attacks. has conducted a cyber espionage campaign against a broad range of victims since at least 2006.
- **China backed threats:** There have been various instances where China-backed states have generated threats in India. For example, a malware was found on one of the systems of Nuclear Power Corporation of India's **Kudankulam plant**. The malware was designed for data extraction and was linked to the **Lazarus Group**, which is **known to have ties to North Korea**.

- **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.

Vulnerable Critical Information Infrastructure

- Recently, there were **cyber-attacks on Kudankulam Nuclear Power Project (KKNPP)**. This has again highlighted the vulnerabilities of our cybersecurity 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 threat**
 - To **identify and reduce the vulnerabilities of individual systems** to any sort of damage or attack and reduce their recovery time.

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.
 - **Indian Cyber Crime Coordination Centre (I4C):** It aims to combat cybercrime in the country, in a coordinated and effective manner. It has 7 components: National Cybercrime Threat Analytics Unit, National Cybercrime Reporting Portal, Platform for Joint Cybercrime Investigation Team, National Cybercrime Forensic Laboratory Ecosystem, National Cybercrime Training Centre, Cybercrime Ecosystem Management Unit and National Cyber Research and Innovation Centre.
 - 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-in 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.

Global measures of Cybersecurity

- **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.
- **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.
- 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.

- **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.
- 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.
 - **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 **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.
- **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.
- **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.
- **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.

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.

1.1. 5G AND CYBERSECURITY

Why in news?

Recently, US formally designated **Huawei Technologies Company and ZTE Corporation**, leading companies in 5G technology research, as “**national security threats**”.

More on news

- There is an apprehension that Huawei Technologies may provide an inner system to enable **surveillance and cyber-espionage for China**. This apprehension is due to following reasons:
 - Both Huawei and ZTE have close ties to the Chinese Communist Party and China's military apparatus, and both companies are **broadly subject to Chinese law obligating** them to cooperate with the country's intelligence services
 - They have been **accused of spying** for Chinese Government by sharing data of foreign citizens.
 - The distrust has further multiplied because of **China's policy to control and dominate** various sectors through its software and hardware systems.
- As a result, many **countries have become sceptical of them**. For instance, France may deter operators from using the Chinese telecom giant's equipment.
- In response to this allegation, **Huawei has criticized** the decision of these governments as political and based on “**ideological prejudices**,” rather than actual security concerns. Also, to counter a D-10 like geopolitical exclusion China has made a proposal to create a ‘BRICS innovation base’ to take forward 5G and Artificial Intelligence (AI) cooperation among the five countries.
- Since there is no hard evidence against Huawei currently, the issue is being linked to the **ongoing trade war between US & China** and has thus sparked a debate between **free commerce and national security**. Taking another geoeconomics turn, the issue has the potential to set off a **technological arms race between US and China**.

India's Position in the debate

- The **Confederation of All India Traders (CAIT)** have asked to **ban Chinese companies Huawei and ZTE** from participating in 5G network roll-out in the country. It also urged that technology and equipment of both companies should be banned from use in 5G network rollout by any company.
- In the context of strained India-China ties, government has been **citing security and strategy related issues** and thus indicating towards exclusion of these firms from the 5G roll-out in India.

How adoption of 5G Technology could generate a cyber security challenge?

5G wireless networks will **connect over 7 trillion wireless devices** serving over 7 billion people, ushering a new era of security threats, which could arise in following forms:

- **Decentralized security needs:** Pre-5G networks had fewer hardware traffic points-of-contact, which made it easier to do security checks and upkeep. 5G's dynamic software-based systems have far more traffic routing points. To be completely secure, all of these need to be monitored.
- **Critical infrastructure protection:** 5G will enable real-time connectivity within critical infrastructure. Thus, any possible weakness in the network security can threaten security of this infrastructure and in turn may threaten our national security.



- **Many IoT devices are manufactured with a lack of security:** As more devices are encouraged to connect, billions of devices with varied security means billions of possible breach points thus increasing overall vulnerability of the system.
- **Network Switching:** Another security risk is posed by **the protocol designed to allow 4G or 3G connections when a dependable 5G signal isn't available.** When a 5G device switches to 3G or 4G, it is exposed to the vulnerabilities that haven't been addressed in the previous generations' protocol.
- **Secure Cloud Computing:** Since cloud computing systems facilitate the sharing of resources among users, it becomes possible for any such user to spread malicious traffic that compromises the performance of the system, to consume more resources, or to gain unauthorized access to the resources of another user.
- **More bandwidth will strain current security monitoring:** While current networks are limited in speed and capacity, this has actually helped providers monitor security in real-time. So, the benefits of an expanded 5G network might actually hurt cyber security.

1.2. ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY

Why in news?

Recent developments like increased use of AI in cyberattacks has showcased how AI can potentially affect National Security.

How use of AI is affecting National Security?

- **Changing nature of security:** The traditional elements of security are rapidly expanding with technological developments leading to creation of newer challenges which are AI dependent.
 - **Rise in frequency and cost of cybersecurity threats:** AI enabled tools have the potential to increase the defensive capabilities of security systems.
 - **Security is growing more complex:** Growth of continuous real-time connectivity, mobile platforms and Internet of Things (IoT) in conjunction with Cyber-Physical systems has made the security landscape more complex.
- **Higher accessibility of AI based tools:** Earlier, the tools and technologies which had security implications like nuclear technology were by and large protected. This ensured that only limited actors had access to such technologies. But same cannot be said for AI because:
 - **Dual-use nature of AI applications:** Many AI applications are dual-use, meaning they have both military and civil applications. This makes **controlling the flow of such technologies extremely difficult.**
 - **Absence of global coalitions for AI based tools on lines of Wassenaar Arrangement or Missile Technology Control Regime (MTCR).**
- **Unavoidable presence of AI:** Artificial intelligence is now touching upon aspects of human life not only in economic domain but also in social domain.
 - **Integration of AI into a product may not be immediately recognizable** i.e. it may not alter the physical structure of a system, but incorporation of AI, changes the overall functioning of the system. For example, it would be very difficult to decipher if a **drone is being controlled remotely or with an AI based system.**

What are the opportunities AI can create vis-à-vis National Security?

- **Increasing real-time intelligence:** AI is expected to be particularly useful in intelligence due to the **large data sets** available for analysis. Large scale structured data combined with the available computational power can generate **significant actionable intelligence.**
- **Creating autonomous and semi-autonomous systems:** These systems collectively increase the geographical reach of the military operations. For example, autonomous systems can be employed to further increase border security without endangering the lives of soldiers.
- **Logistical ability:** AI may have future utility in the field of **military logistics.** For instance, it can ensure continuous observation of border infrastructure and provide intelligent inputs with respect to need for repairs.
- **Cyber operations:** AI is likely to be a key technology in advancing military cyber operations both in offensive and defensive capacity.

- **Replacing humans in ‘dull, dangerous or dirty’ work:** Depending on the task, autonomous systems are capable of augmenting or replacing humans, freeing them up for more complex and cognitively demanding work. For example, AI can be used in conducting long-duration intelligence collection and analysis or cleaning up environments contaminated by chemical weapons.

What are the steps taken by India to tap this opportunity?

In 2018, government constituted a **task force under Natarajan Chandrasekharan** comprising representatives from the government, services, academia, industry, professionals and start-ups to prepare a road map for Artificial Intelligence for national security purposes.

The Government accepted majority of its recommendations in 2019, thus creating **an institutional framework for adoption of AI in National Security**. Following can be cited as key facets of this framework:

- **Defense AI Council (DAIC):** A high-level DAIC has been created under the chairmanship of Defense Minister with following responsibilities:
 - Provide **strategic direction towards AI driven transformation** in Defense.
 - Provide guidance and **addressing issues related to data sharing**.
 - Provide guidance in building **strategic partnership with industry**.
 - Review recommendations concerning **acquisition of technology and startups**.
 - Review the **ethical, safe, secure and privacy** assured usage of AI in defense.
 - Set policies in partnership with government institutions and industries to **create deterrent for social and technology misuse**.
- **Defense AI Project Agency (DAIPA):** It also envisages to establish a DAIPA with Secretary (Defense Production) as its ex-officio Chairman. The key responsibilities of DAIPA will be to-
 - Evolve and adopt a **preferred technology stack within Defense establishments** for development of AI Use Cases.
 - Evolve and **adopt standards for technology development** and delivery process for AI projects.
 - Formulate policy for **Intellectual Property Rights (IPR)**.
 - **Enable and review** the delivery of AI projects.
 - Incentivize the use of AI in existing systems and processes that demonstrate operating benefits.
 - Formulate policy for selection of, and contractual engagement with **strategic industry partners**.
- **Integration of AI into India’s Defense Strategy:** All organizations in Ministry of Defense have been asked to integrate and embed AI, in an appropriate manner, in their strategies. These include the three Services, the Coast Guard, DRDO and DPSUs among others.

Centre of Artificial Intelligence and Robotics (CAIR)

- It is **laboratory of the Defense Research and Development Organization (DRDO)**. CAIR is the primary laboratory for R&D in different areas of **Defense Information and Communication Technology (ICT)**.
- It has a **comprehensive library for AI-based algorithms** and data mining toolboxes that can potentially be used for image/video recognition, Natural Language Processing (NLP), swarming (learning from observing nature and applying the concepts to machines).

What are the potential challenges in adoption of AI for National Security?

- **Absence of clarity on ‘what is AI’ and ‘what we intend to do’ among policymakers:** There is a limited understanding of key questions like- What kind of AI do we want? How much autonomy should be given to the machines on the battlefield? Etc.
- **Development of Ethical Standards:** Use of AI in defense would raise a large number of ethical questions like- Who holds the accountability in case AI does not perform as predicted? How can AI be integrated with current protocols followed in the forces? How far AI can be trusted for the protection of the country? Development of these ethical standards is a prerequisite for adoption of AI for National Security.
- **Theft vulnerability:** AI systems are particularly vulnerable to theft by virtue of being almost entirely software based.
- **Technology cannot be completely controlled:** Using AI systems can significantly increase the scale and speed at which military operations are conducted. If the pace of operations exceeds human ability to understand and control events, that could **increase a system’s destructive potential in the event of a loss of system control**.
- Other issues like **limited role of private sector in defense** and **lack of critical infrastructure**.

What can be done to overcome these challenges?

- **Vision document on AI:** India should envisage a clear strategic vision regarding the AI. Having a Vision document provides clarity to policymakers as well as the defense establishments regarding capabilities and envisaged outcomes.
- **Creation of a supportive ecosystem:** Along with a clear policy, there is a dire need to **invest in critical infrastructure** so that the data servers lie within the territory.
- **International cooperation:** To ensure that India is at par with other countries with regard to adoption of AI in National Security, various efforts like joint development, technology sharing, encouraging development of global policy and standardization could be done.
- **Tapping the civilian innovation ecosystem:** The AI-market for civilian purposes in the country is on the rise. For instance, India ranks third in G20 countries in AI-based startups. Policymakers could tap this potential for the defense sector.
- **Balancing adoption and innovation:** Since India is a late entrant in the field vis-à-vis powers like China and US, it could capitalize on the late-movers advantage, i.e., **mimicking the existing narrow-AI technologies**, to fulfil its basic security needs (like border patrols and intel-gathering) alongside **innovating over and above the existing technologies**.

1.3. FAKE NEWS

Why in news?

Recently, misinformation circulating on social media, fuelling public fears around coronavirus, and the tendency of **mass-forwarding messages** without verifying content has once again brought the issue of fake news into the mainstream.

About Fake News

- Fake news is defined as “information that is likely to be perceived as news, which has been **deliberately fabricated** and is disseminated with the intention to deceive others into believing falsehoods or doubting verifiable facts”.
- A Microsoft study found that over **64% Indians encountered fake news online, the highest reported among the 22 countries surveyed**.

Causes responsible for developing fake news culture

- **Increasing mobile and internet penetration:** India has the most social media users, with 300 million users on Facebook, 200 million on WhatsApp and 250 million using YouTube.
- **Emphasis on likability enhancement of the news:** Social media algorithms are geared to appeal to people’s habits and interests and the emphasis is on **likeability, and not accuracy**.
- Fake news is being used as an extension of propaganda and advertising. Unlike the traditional process, there are **no editorial controls or quality-assurances**.
- **Lack of comprehensive legislation:** There is **no specific law to deal with fake** newsmakers which allows miscreants to take undue advantage of the situation as authorities mostly remain confused as to the actionable wrong.

Challenges posed by the Fake News

- **Weakens the democracy:** Fake news poses a serious challenge to this proposition as it misleads the consumers of information, poses a threat to a democratic society as it can give a handle to the state to interfere with the functioning of media.
 - **For instance**, Facebook took a hammering over Russia's interference in the 2016 U.S. election. It conceded the following year that up to 10 million Americans had seen advertisements purchased by a Russian agency.
- **Affecting choices and behaviours:** These platforms are predominant source of news and a critical mass of misinformation leads to mis-directed behaviours filled with fake news and disinformation aimed at influencing choices ranging from day to day life to political choices made during the Indian elections.
- **Threat of infodemic:** The WHO warns that societies around the world are facing an “**infodemic**”—an “**overabundance**” of information that makes it difficult for people to identify truthful and trustworthy sources from false or misleading ones.

- **Give rise to various crimes:** Crimes that includes communal riots, mob lynching, mass hysteria, etc. are many times the product of fake news being shared by the people.
- **Violates rights of the citizen:** The boundless dissemination of fake news on the social media induces crime against humanity and infringement of citizens' right to unbiased and truthful news and reports.
- **Affecting the economy at large as we witnessed that how** the misinformation pandemic has also pervaded industries altogether unrelated to COVID-19 infection, such as **poultry and seafood sector**.
- **Spread hatred and mistrust:** False information propagated through fake news have helped people developing racist and xenophobic sentiments against people of Asian origin around the world, as we saw in the case of Corona epidemic. Such messages can often be a means of **reinforcing existing prejudices**.
- **Influences the mainstream information dissemination mechanism:** Fake news disrupt the traditional or official chain of information.
 - For instance, the official agency, Press Information Bureau has also drawn criticism for advocating treatments offered by alternative medicine systems without any supporting **scientific evidence and or clinical testing data**.

Measures taken to curb the menace of Fake News:

- **Legislations:**
 - **Section 505(1) of Indian Penal Code, 1860-** whoever by making, publishing or circulating any statement, rumour or report which may cause fear or alarm to the public, or to any section of the public shall be punished with imprisonment which may extend to three years, or with fine, or with both.
 - **Section 66D of Information Technology Act, 2000-** Whoever, by means for any communication device or computer resource cheats by personating shall be punish with the imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.
 - **Section 54 of the Disaster Management Act, 2005:** Whoever makes or circulates a false alarm or warning as to disaster or its severity or magnitude, leading to panic shall be punishable with the imprisonment which may extend to one year or with fine.
- **By the Government:**
 - In the current wake of Corona epidemic, Government initiatives like **the introduction of an official chatbot on WhatsApp** named **'MyGov Corona News Desk'** which answers queries about the virus with an aim to prevent spreading of rumours during this pandemic.
 - The Press Information Bureau (PIB) has created a fact checking unit in order to tackle the fake news on social media targeting the government and the work being done by it.
- **Initiatives taken by social media intermediaries:**
 - Facebook has developed **an Artificial Intelligence system that can investigate** and deactivate fake accounts disseminating fake news.
 - **Facebook's fact checking program**, under which content rated false is downgraded in news feeds so that fewer people see it.
 - WhatsApp recently partnered with the World Health Organisation (WHO), United Nations Children's Fund (UNICEF), and United Nations Development Programme (UNDP) to launch **WhatsApp Coronavirus Information Hub**.
- **By the Election Commission of India**
 - In the **lead-up to the elections**, the ECI, summoned the top executives of Facebook and Twitter to discuss the crisis of coordinated misinformation, fake news and political bias on their platforms.
- **Supreme Court on Fake News:**
 - As per the court, media should maintain **a strong sense of responsibility**, while disseminating news and should ensure that unverified and fake news is not published.
 - **In case of recent Corona epidemic**, as per Supreme Court, media should **refer to and publish the official version about developments regarding coronavirus** threat, the court said, while maintaining that it does not intend to interfere with the "free discussion" about the pandemic.
- **Role of Media:** Various media outlets are taking initiatives to fact check the information being shared.

Way Ahead

- **Promoting the culture of self-verification:** Where people who consume the data on an everyday basis educate themselves and acquire the skills to tackle it. Thus, there is a need to shift towards a system where self-verification of information is an ‘internet skill’ and an important duty.
 - This can be done simply by a quick search on Google or checking for that information or visiting the official websites to verify the accuracy of the data.
- **Responsible citizenry:** Consumers who play the central role in the spread of misinformation, are also the **most efficient and effective in debunking the various myths and fake news.** This skill can be taught via:
 - creating **awareness** on television and social media, or
 - innovative initiatives like ‘Fake News Classes’ introduced in government schools in Kerala, where they teach students how to identify and spot misinformation.
 - by **asking questions** like “What is the source of that (post/forward)?”

“You are as strong as your Foundation”

FOUNDATION COURSE GENERAL STUDIES PRELIMS CUM MAINS 2021

Approach is to build fundamental concepts and analytical ability in students to enable them to answer questions of Preliminary as well as Mains examination

- Includes comprehensive coverage of all the topics for all the four papers of GS Mains, GS Prelims & Essay
- Access to LIVE as well as Recorded Classes on your personal student platform
- Includes All India GS Mains, GS Prelims, CSAT & Essay Test Series
- Our Comprehensive Current Affairs classes of PT 365 and Mains 365 of year 2021

ONLINE Students
NOTE - Students can watch LIVE video classes of our COURSE on their ONLINE PLATFORM at their homes. The students can ask their doubts and subject queries during the class through LIVE Chat Option. They can also note down their doubts & questions and convey to our classroom mentor at Delhi center and we will respond to the queries through phone/mail.

DELHI
Regular Batch: **25 Nov 10 AM**
Weekend Batch: **27 Oct 5 PM** | **21 June 9 AM**

27 Oct | JAIPUR | AHMEDABAD | HYDERABAD | PUNE

CHANDIGARH | **7 Aug**
LUCKNOW

LIVE/ONLINE CLASSES ALSO AVAILABLE

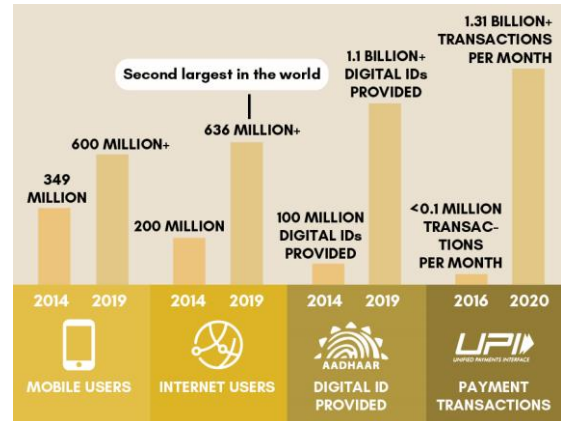
2. DATA PROTECTION

Introduction

Data is considered a **national resource** that should be utilized for the welfare of the society. With the exponential growth in generation as well as usage of data, it is extremely essential that this usage is done in secure framework. This security encompasses individual security, personal privacy, security for businesses and national security.

The need for data protection

- **Protection of privacy:** India has more than 62 crore internet users, whose personal data is shared online. With supreme Court declaring Right to Privacy a Fundamental right (**K.S. Puttaswamy** case) protecting individual privacy is constitutional duty of the state.
- **Check snooping or surveillance by various agencies:** Recently, 121 Indian citizens' WhatsApp accounts were hacked by an Israeli software called Pegasus.
- The **Facebook–Cambridge Analytica data scandal of 2018** where personal data of millions of peoples' Facebook profiles without their consent was used for political advertising purposes.
- **Economic losses:** The average cost of data breach in India is Rs 12.8 crore, with per capita cost per lost or stolen record reaching Rs 5,019 in 2018, as per a study by IBM.
- Moreover, data is being considered as new oil in 21st century. Without proper data regulations or data localisation norms, Global firms like Google, Face book are benefitting from data collected from Indians.
- **Increasing sophistication of cyber-crimes:** The root cause for 51 per cent of data breaches was malicious or criminal attacks, in India as per IBM study.



What is the current framework for Data Protection in India?

- **Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011** is referred to, for **general application** with regard to privacy laws.
- **Collection of Government Data** is governed by Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 and **Aadhaar (Data Security) Regulations, 2016**.
- **Data related to the Banking Sector** is regulated under Credit Information Companies (Regulation) Act, 2005, Credit Information Companies Regulations, 2006, circulars of Reserve Bank of India including KYC circulars, Master Circulars on credit cards and Customer Services and Code of Bank's commitment to Customers.
- Data related to the **healthcare sector** is regulated by **Clinical Establishments (Central Government) Rules, 2012** and **Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002**.
- As part of potential reforms with regard to the Data Protection regime, **Personal Data Protection Bill, 2019** (currently referred to the standing committee), **Non-Personal Data Governance Framework** and **National Digital Health Mission** among others have been envisaged.

Draft Data Empowerment and Protection Architecture

Recently, **NITI Aayog** sought suggestions and comments on the 'Data Empowerment and Protection Architecture (DEPA)' draft. **Data protection should be complimented with data empowerment** in order to **prevent financial exclusion**, for **utilization of emerging large-scale data** and from **preventing data from remaining in Silos**.

What is Data Empowerment?

Data empowerment is the **process where people**, on their own or with the help of intermediaries, **take control** or gain the power to take control **of their data** to **promote their and their society's wellbeing**. For this, people need to

- **be aware of how their data is used.**
- have a **right to privacy** and able to exercise it.
- be able to **demand disclosure of data** about key issues of interest, and use it to **hold institutions accountable**.
- have the **right to create and produce data**, and **use it for the common good**.

Salient features of the draft Data Protection and Empowerment Architecture (DEPA)

- **DEPA will act as final layer of India Stack:** India Stack is a privately-owned bouquet of proprietary software or APIs powering Aadhaar-based applications, and UPI based digital transactions. It allows government, businesses to use India's digital infrastructure to deliver private services.



- **Organization-centric system to individual centric system:** The policy aims to work on the ideology that individuals themselves are the best judges of the 'right' uses of their personal data.
- **Consent Managers:** In view of the treatment of personal data as an economic good, the policy advocates for the creation of "a new class of institutions" called 'consent managers' that will act as a conduit between stakeholders.
- **Technological Architecture:** It creates interoperable, secure, and privacy preserving digital framework for data sharing.

What are the constraints in data protection?

- Most of the **data storage companies are based abroad**. They also export data to other jurisdiction making it difficult to apply Indian laws.
- **Multiple private players are involved in data dynamics** which makes it difficult to apply uniform data protection framework.
- Generally, the **application using pre-ticked boxes on consent** while asking users regarding the acceptance to the terms and conditions, leads to uninformed consent.
- It is usually **difficult to trace the perpetrator invading the data privacy**.

2.1. THE PERSONAL DATA PROTECTION BILL, 2019

Why in news?

Recently, the **Personal Data Protection Bill, 2019** was introduced in Lok Sabha.

Key features of the Bill

- **Personal data (data that can identify an individual):** The bill talks about various types of personal data, such as **Sensitive personal data, Critical personal data** and **General personal data**.
- **Applicability:** The Bill governs the processing of personal data by Government, companies incorporated in India and foreign companies dealing with personal data of individuals in India.
- **Obligations of data fiduciary (an entity or individual who collects and decides the means and purpose of processing personal data):**
 - Personal data can be processed only for **specific, clear and lawful purpose**.
 - All data fiduciaries must undertake certain transparency and accountability measures such as implementing security safeguards (such as **data encryption and preventing misuse of data**) and instituting **grievance redressal mechanisms** to address complaints of individuals.
- **Rights of the data principal (the individual whose data is being collected and processed):** These include the right to:
 - **obtain confirmation from the fiduciary** on whether their personal data has been processed
 - restrict continuing disclosure of their personal data by a fiduciary, if it is no longer necessary or consent is withdrawn. It also includes the **right to be forgotten** which will allow users to erase their personal data published online.
- **Grounds for processing personal data:** The Bill allows processing of data by fiduciaries only if consent is provided by the individual.
- **Social media intermediaries:** platforms with larger number of users and having potential to impact electoral democracy or public order, have certain obligations, which include providing a voluntary user verification mechanism for users in India.
- **Data Protection Authority:** The Bill sets up a Data Protection Authority which may take steps to protect interests of individuals, prevent misuse of personal data and ensure compliance with the Bill.
- **Transfer of data outside India:**
 - **Sensitive personal data** may be transferred outside India for processing if explicitly consented to by the individual and subject to certain additional conditions. However, such sensitive personal data should continue to be stored in India.
 - **Critical personal data** can only be processed in India.
 - **Personal data other than sensitive and critical personal data** don't have such localisation mandates.
- **Sharing of non-personal data with government:** The central government may direct data fiduciaries to provide it with any non-personal data and anonymized personal data for better targeting of services.

Criticisms of the bill

- There are **significant departures** in the current bill from the draft Bill prepared by the Justice **B N Srikrishna committee** in 2018.
 - **Data Protection Authority's composition** is dominated by the government, as contrasted with the diverse and independent composition as suggested in the committee's draft.
 - There is a **blanket power of exemption** from all provisions of the law (including access to personal data without consent, citing national security, investigation and prosecution of any offence, public order) in favour of a government agency.
- A report from the IT Ministry's Artificial Intelligence (AI) Committee contradicts some foundational aspects of the Bill, as it suggests:
 - **India should maintain free flow of data** stating that India has been one of the biggest beneficiaries of the global data flows. Limitations on the free and open flow of data can seriously hinder the **ability of economy** to remain competitive.
 - **Focus should be placed on implementation and enforcement** instead of over-regulation. **Sectoral entities are more appropriate regulators** than an overarching authority.
 - Legislation alone is not enough unless supported by an **adequate implementation ecosystem including an effective grievance redressal system and user awareness**.

2.2. NON-PERSONAL DATA

Why in news?

The draft report on **Non-Personal Data (NPD) Governance Framework** was released recently for inviting feedbacks by the committee **headed by Kris Gopalakrishnan**.

What is Non-Personal Data?

- The draft report defines non-personal data as any **set of data which does not contain personally identifiable information**, in essence means that no individual or living person can be identified by looking at such data.
- **Difference from personal data:**
 - Unlike personal data, which contains explicit information about a person's name, age, gender, sexual orientation, biometrics and other genetic details, **non-personal data is more likely to be in an anonymised form**.
 - Anonymous data is a data that is **initially personal data but is later made anonymous using certain data transformation techniques**, to the extent that individual specific events are no longer identifiable.
- **Classifications of non-personal data:** The draft report classifies NPD as:
 - **Public non-personal data:** All the **data collected by government and its agencies** such as census, data collected on the total tax receipts or any information collected during execution of all publicly funded works has been kept under the umbrella of public non-personal data.
 - ✓ While **Non-Personal Data collected or generated by the Government where such data is explicitly afforded confidential treatment under a law**, like data of land records, public health information, vehicle registration data **shall not constitute Public Non-Personal Data**.
 - **Community non-personal data:** Any **data identifiers about a set of people** who have either the same geographic location, religion, job, or other common social interests will form the community non-personal data.
 - ✓ E.g. the metadata (set of data that describes and gives information about other data) collected by ride-hailing apps, telecom companies, electricity distribution companies.
 - **Private non-personal data:** It can be defined as those which are produced by individuals which can be derived from application of proprietary software or knowledge. Private non-personal data is further sub-classified into 'sensitive non-personal data' & 'critical non-personal data'.

Why there is need to regulate Non-Personal Data (NPD)?

- **Sensitivity of data:** Like personal data NPD can also sensitive if it relates to national security or strategic interests, it contains business sensitive or confidential information or it is anonymized data, that bears a risk of re-identification.
- **Rights of citizens over NPD:** Regulation will ensure a community's rights over the community Non-Personal Data.



- Law must assure that the rights of citizens to the protection of their personal data are always respected, including when their data are properly anonymized.
- **Regulate digital industry:** Organizations have been discovering newer ways to generate value from data and possibility of data monopolies has led to **outsized benefits and create a certain imbalance in the data and digital industry.**

Other recommendations of the report:

- **Stakeholders and their roles:** It recognizes natural persons, entities and communities to whom non-personal data (prior to anonymization or aggregation) relates as **'data principals'** and entities which undertake collection, storage and processing of non-personal data as **'data custodians'**.
- **Requirement of consent:** It classifies individuals to whom the data relates (prior to anonymization), as the 'owners' of private non-personal data and it recommends obtaining consent of the data principal (at the time of collection) for anonymization and use thereafter.
- **Localization of data:** It recommends localization of sensitive non-personal data and critical non-personal data.
- **Purpose of data sharing:** The Report contemplates three broad purposes for data sharing:
 - **for sovereign purposes may be used by the Government,** regulators and law enforcement authorities, inter alia, for cyber security, crime and investigation, public health and in sectoral developments.
 - **for core public interest purposes** may be used for general and community use, research and innovation, delivery of public services, policy development etc.
 - **for economic purposes may be used by business entities** for research, innovation and doing business. It may also be leveraged as training data for AI/ML systems.
- **Non-Personal Data Authority (NPDA): to be created** for the collection, processing, storage and sharing of NPD.
- **Creation of a Non-Personal Data Policy Switch as a single digital clearing house:** To address issues around conflicting rules of data trustees over the same body of non-personal data, the report proposes a digital Non-Personal Data Policy Switch.
- **Promote research:** The Report also recommends establishments of data spaces, data trusts and cloud innovation labs and research centers which may act as physical environments to test and implement digital solutions and promote intensive data-based research.
 - The government needs to **improve on Open Government Data initiatives** and make high-quality public non-personal datasets available. Moreover, data sharing principles must be applied uniformly to all three categories of non-personal data.

2.3. SECURITY ISSUES WITH AAROGYA SETU APP

Why in news?

Recently, some experts have raised **privacy and security concerns** with the Aarogya Setu app launched by the Government of India.

Concerns with app

- **Security issues-** Recently, some individuals and groups on social media claimed that they were able to access information about people who were infected by coronavirus, among other data points, including people in sensitive offices like the PMO or Parliament.
 - Government has clarified that the app fetches users data and **stores it on the server in a secure, encrypted, anonymised manner** only at the time of registration and self-assessment.
- The **privacy policy of the app is silent** on as to what security practices are being followed and what level of encryption is being used.
 - Although, to showcase the transparency in the structure of the application, Government has made the **source code of the Aarogya Setu app open source.**
- **Violates constitution-** As per the Supreme Court, privacy is a fundamental right, and it can only be deprived in accordance with procedure established by the law. There is no act passed by the parliament, which authorises the mandatory nature of the app.
- **Lack of accountability-** The app has a clause, which limits the government's liability, in case of any unauthorised access or modification to the information provided by the user. This means that there is no liability for the government even if the personal information of users is leaked.

- **Legally unjustified** - By limiting the government's liability, the app goes against the **Information Technology Act** and the proposed **Personal Data Protection Bill**. The reasons for this is that the app service provider would fall under the **definition of an intermediary** and is obligated to ensure the security of the data collected and is liable for loss of it under the intermediary guidelines.
- **Apprehensions over its creation:** The National Informatics Centre (NIC), which designs government websites said to an RTI reply that it has no information about who has created the Aarogya Setu app. But the Aarogya Setu's website shows that it has been developed by NIC and the IT Ministry.
 - As a clarification, the Government has reiterated that the app has been **developed by NIC and IT Ministry along with Private players**.

Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020

- **Implementation of the Protocol:** MeitY is designated as the agency responsible for the implementation of this Protocol and its developer, the National Informatics Centre shall, under this Protocol be responsible for collection, processing and managing response data collected by the Aarogya Setu mobile application.
- **Collection and processing of response data:** Any response data and the purpose for which it is collected by NIC shall be clearly specified in the Privacy Policy of the Aarogya Setu mobile application.
- **Demographic data will be retained for as long as Protocol remains in force** or if **individual requests that it be deleted, for a maximum of 30 days** from such request, whichever is earlier.
- **Sharing of response data:** Data can be shared with other government agencies and third parties as long as it is for critical health purposes.
- **Response data may be made available for research purposes** to Indian universities and research institutions/ research entities registered in India by NIC.
- **Any violation of these directions may lead to penalties** as per Disaster Management Act, 2005 and other legal provisions as may be applicable.
- **The Empowered Group shall review this Protocol** after a period of 6 months from the date of this notification or may do so, at such earlier time as it deems fit.

Way Forward

- The government should keep **refining both the product and the policy**, with the understanding of the pandemic and the privacy dangers posed by such an app.
- The government can take a cue from countries like **South Korea** and **Singapore**, who have enacted privacy laws that have specific conditions for contact tracing apps developed to track the spread of the pandemic.

फाउंडेशन कोर्स सामान्य अध्ययन प्रारंभिक एवं मुख्य परीक्षा 2021

इनोवेटिव क्लासरूम प्रोग्राम

- प्रारंभिक परीक्षा, मुख्य परीक्षा और निबंध के लिए महत्वपूर्ण सभी टॉपिक को विस्तृत कवरेज
- मौखिक अवधारणाओं, की समझ के विकास एवं विरलेषणात्मक क्षमता निर्माण पर विशेष ध्यान
- एनीमेशन, पॉवर प्वाइंट, वीडियो जैसी तकनीकी सुविधाओं का प्रयोग
- अंतर - विषयक समझ विकसित करने का प्रयास
- योजनाबद्ध तैयारी हेतु करंट ओरिएंटेड अप्रोच
- नियमित क्लास टेस्ट एवं व्यक्तिगत मूल्यांकन
- सीसेट कक्षाएं
- PT 365 कक्षाएं
- MAINS 365 कक्षाएं
- PT टेस्ट सीरीज
- मुख्य परीक्षा टेस्ट सीरीज
- निबंध टेस्ट सीरीज
- सीसेट टेस्ट सीरीज
- निबंध लेखन - शैली की कक्षाएं
- करंट अफेयर्स मैगजीन

लॉकडाउन तक कक्षाएं ऑनलाइन होंगी। लॉकडाउन के बाद, ऑफलाइन कक्षाएं शुरू की जाएंगी।

DELHI 29 OCTOBER | 1:30 PM
LUCKNOW 15 SEPT | 9 AM **JAIPUR 15 SEPT | 4 PM**

लाइट/ऑनलाइन कक्षाएं भी उपलब्ध

3. BORDER SECURITY AND MANAGEMENT

Introduction

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. Thus, it becomes important that we develop capabilities to protect our border areas in varied terrains, with multiple countries with whom we have very different security relationships.

Issues related to Border management in India

- **Porosity of borders:** International borders with Pakistan and Bangladesh run through diverse terrain including deserts, marshes, plains and mountains.
 - This porosity of borders facilitates various illegal activities such as smuggling, trafficking of humans, drugs and arms and infiltration.
- **Contested International borders:** History of mistrust and constant border skirmishes with Pakistan along line of control (LOC) makes India highly susceptible to cross-border terrorism.
 - Similarly, India's border with **Myanmar** is **threatened by several insurgent groups** that have **found sanctuaries in jungles** along the border.
 - Political boundary issues of **“enclaves and adverse possessions”** in **Bangladesh** have resulted in political sensitivity along the entire eastern border.
- **Inefficiency in Border management:** Indian borders continue to be guarded by military and police forces that report to different ministries in the Centre and states, making the border management task arduous and leading to duplication of efforts by the security forces.
- **Lack of critical infrastructure:** Critical infrastructure such as observation towers, bunkers, Border Flood Lights etc. are lacking in many border areas which also prevent deployment of hi-tech equipment.
- **Poor intelligence and resource efficiency:** Security forces are ill-equipped to handle border management given poor intelligence capabilities and severe resource deficiency.
- **Ethnic conflicts and separatist movements:** The situation has worsened due to the changed demographic profile of many Border States and shift in ethnic balance of communities as a result of illegal migration.
- **Over-population in the border areas:** Density of population in the border areas at some places is approximately 700-800 persons per square km on the Indian side and about 1,000 persons on the Bangladesh side.
- **Political instability and disorder** in its periphery impacts India's security directly or indirectly. Proxy war between India and Pakistan adds to this security risk.

Technology can play an integral role in addressing Border Management Issues

- **Upgrading existing system:** Technology can be integrated with the existing systems to facilitate better detection and interception by the man behind the machine.
 - At present, border guarding is **almost fully dependent on human surveillance**. This makes border management a time-consuming and complex task.
- **Checking infiltration:** It can be 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.
- **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 allterrain and all-weather inputs.
- **Madhukar Gupta Committee on border protection** had recommended the Union Government to **strengthen border protection and address vulnerabilities in fencing** along the Indo-Pakistan border. This led to **implementation of CIBMS in 2015**.

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 improves the **capability of Border Security Force (BSF) in detecting and controlling the cross border crimes** like illegal infiltration, smuggling of contraband goods, human trafficking and cross border terrorism etc.

- It also **improves situational awareness** to facilitate prompt decision making and quick reaction to emerging situations.
- It involves deployment of **a range of state-of-the-art surveillance technologies**.
- 2 pilot projects covering about 71 Kms on Indo-Pakistan Border (10 Kms) and Indo-Bangladesh Border (61 Kms) of CIBMS have been completed.
- In 2018, BSF undertook the project **BOLD-QIT (Border Electronically Dominated QRT Interception Technique)** to equip Indo-Bangladesh borders with different kind of sensors in unfenced riverine area of Brahmaputra and its tributaries.

Steps that can be taken further

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

3.1. BORDER INFRASTRUCTURE

Why in news?

Recently, Government accepted and implemented three important recommendations of Shekatkar Committee relating to border Infrastructure.

Three recommendations were related to **speeding up road construction**, leading to **socio economic development in border areas**. They were:

- **Outsourcing road construction work** beyond optimal capacity of Border Roads Organisation (BRO). **Engineering Procurement Contract (EPC) mode is made mandatory** for execution of all works **costing more than Rs 100 crore**.
- Introduction of **modern construction plants, equipment and machinery** by delegating **enhanced procurement powers** from Rs 7.5 crore to Rs 100 crore **to BRO, for domestic and foreign procurements**.
- **Land acquisition and all statutory clearances** like forest and environmental clearance are made **part of approval of Detailed Project Report**. Work can be awarded only after at least 90% of statutory clearances have been obtained.

Need for Border infrastructure

- **Imperative to National security**: India's border is vulnerable to political instability, cultural radicalism and patronage of terrorism arising from the neighbouring countries.
- **Matching Neighbouring countries' Infrastructure** along the border like that of China's. It laid roads, railway line, and communication network, including fibre optics along the border.
- **For developmental needs and well-being of people living in border areas**.
- **Tactical and strategic mobility** is impeded by lack of Infrastructure resulting in predictability of operations.
- **For facilitation of legitimate trade and travel** along with supervision to control smuggling, trafficking, crime, terrorism and illegal migration can increase.

Limitation in developing border infrastructure

- **Poor implementation**: In 2017, CAG pointed out that of the **73 roads allotted** in border areas, only 22 roads were completed by March 2016. Similar was the case with **14 strategic railway lines**.
- **Lack of monitoring** resulting in **defective construction of roads** including faulty design, poor riding conditions, inadequate drainage facilities etc.

- **Multiple authorities managing the border:** India has Army, Indo-Tibetan Border Police, Border Security Force and Assam Rifles for border management, unlike China which has one command for its security forces managing border, indicating cohesiveness.
- **Lack of unity of command:** Management becomes slightly inefficient because in some places the **Ministry of Home Affairs (MHA)** is responsible and in other places the **Ministry of Defence (MoD)** is responsible.
- **Staff deficiency and lack of modern equipments:** BRO is battling staff deficiency, lacks skilled workforce, too much dependence on local contractors.
- **Lack of adequate allocation of funds** for infrastructure, even pointed out by army.

Steps taken

- **Border Area Development Programme (BADP):** Main objective of the BADP is to meet the special developmental needs and well-being of the people living in areas situated near the International Boundary (IB).
- **Border Infrastructure and Management (BIM)** which includes 60 projects like construction of roads, schools, primary health centers, helipads, promotion of border tourism etc.
- **Completion of Indo-China Border roads:** Of 61 roads planned in 1st phase, 36 have been constructed.
- **Expediting forest clearances:** For taking up border infrastructure works, Government accorded **General approval under Forest (Conservation) Act, 1980.**
- Creation of **National Highways & Infrastructure Development Corporation Limited (NHIDCL):** NHIDCL took over several projects from BRO to address delay in execution.

3.2. CHALLENGES IN BORDER AREAS AND RECENT INITIATIVES TO TACKLE THEM

Border	Challenges along the border	Recent initiatives by government
Sino-India	<ul style="list-style-type: none"> • Border dispute at Aksai Chin, Arunachal Pradesh, Doklam etc. with sporadic aggression. • Large scale smuggling of Chinese electronic and other consumer goods take place through these border points even after designated areas for border trade. • 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. • Multiple forces along Indian border (for e.g.- ITBP, Assam rifles, Special frontier force) as opposed to single PLA commander on Chinese side. • Water-sharing issue as China is building dams on its side reducing water flows on our side. 	<ul style="list-style-type: none"> • Creating infrastructure: India is also constructing some critical bridges to cut down time for troop movement such as Dhola- Sadiya bridge. • India has joined hands with Japan to aggressively develop infrastructure projects in North east to contain China. • Army infrastructure projects within 100 Km of LAC have been exempted from forest clearance. • To expedite border road construction, Ministry of Defence has decided to delegate administrative and financial powers to the Border Roads Organisation (BRO).
Indo-Pak	<ul style="list-style-type: none"> • Border dispute at Sir Creek and Kashmir. • River water sharing issue at Indus river. • Infiltration and Cross-border terrorism. targeted to destabilize India. Recently BSF detected a fifth (since 2012) cross- border tunnel in the forest area of Jammu. • Diverse terrain including desert, marshes, snowcapped mountain and plains makes border guarding difficult. • Time & cost overruns in infrastructure projects due to unforeseen. circumstances& natural calamities. • Other issues include drug smuggling, fake currency, arms trafficking. 	<ul style="list-style-type: none"> • Following Pathankot terrorist attack, MHA sanctioned implementation Comprehensive Management System (CIBMS) to establish an integrated security system at borders providing all-round security even in adverse climatic conditions. • 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 police and other paramilitary forces in room intervention, anti-terror skills, overseeing anti-hijack operations etc.

Indo- Nepal	<ul style="list-style-type: none"> Increasing Extremism and anti-India activities due to increasing activities of ISI such as pushing in men and explosives through the border. Fear of spread of Maoist insurgency due to links of Nepal's Maoists in India. Easy escape & illegal activities - Insurgents, terrorists, many hard-core criminals pursued by Indian and Nepalese security forces escape across the open border. <ul style="list-style-type: none"> 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. Other issues: Disputed border at times lead to land grabbing on each side. 	<ul style="list-style-type: none"> Establishment of a new intelligence section in SSB at Indo-Nepal and Indo-Bhutan border to ensure better operational efficiency. Establishment of Border District Coordination Committee at the level of district officials of the two countries to discuss issues of mutual concern. The Government of India has approved construction of 1377 km of roads along Nepal border. Development aid to Nepal to prevent human trafficking owing to lack of employment opportunities there.
Indo- Bhutan	<ul style="list-style-type: none"> Insurgency- Many groups such as Bodo, ULFA etc. sneak into Bhutan for sanctuary despite their army driving them out. Smuggling of goods such as Bhutanese cannabis, liquor and forest products. Free movement of people and vehicle leading to issues such as during the Gorkhaland movement in West Bengal. 	<ul style="list-style-type: none"> Bilateral cooperation - A Secretary level bilateral mechanism in the shape of an India- Bhutan Group on Border Management and Security. Cooperation with their army to prevent sanctuary to insurgents in their soil. Establishing new border posts in Sikkim along the Bhutan frontier near Doklam. 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	<ul style="list-style-type: none"> Free movement Regime: Insurgents are misusing FMR to cross-over to Myanmar and receive training and acquire arms. Drug trafficking due to proximity to golden triangle. 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. Poor Infrastructural facilities at Moreh and Zokhawatar – the two designated points for normal trade and border trade. 	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Water disputes such as sharing of Teesta river, construction of Dam by India on Barak river. 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. <ul style="list-style-type: none"> Rohingya crisis (religious persecution) has also added to it as 40,000 rohingya refugees were estimated in India in 2017. Inadequate border fencing due to issues such as riverine areas, protests by residing population, pending land acquisition etc. Trafficking of goods like jamdani sarees, rice salt etc. as well as cattle smuggling. 	<ul style="list-style-type: none"> India Bangladesh Land Boundary Agreement, 2015. Government has announced the establishment of Border Protection Grid (BPG) with Indo- Bangladesh Border States. 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. Installation of Border surveillance devices such as closed-circuit cameras, search- lights, thermal imaging devices and drones to keep a tight vigil. The BSF and BGB have also been raising awareness among the locals regarding crime prevention in the border area.

4. EXTREMISM AND TERRORISM

Introduction

Extremism in the context of security implies adoption of illegal and violent ways to propagate one's ideology. Extremists are motivated by different goals and objectives. Depending on the objectives of the group/groups, the nature of terrorism also differs such as ethno-nationalist terrorism, religious terrorism, left-wing terrorism, right-wing terrorism, state sponsored terrorism, cyber terrorism, urban terrorism etc.

What are key elements of a potential counter-terror strategy?

- **Political consensus:** Union Government should have intensive interactions with the States and Union Territories while drawing up the national strategy, the latter would be required to do their part in close consultation with the nodal ministry of the Government of India.
- **Good governance and socioeconomic development:** This would necessitate high priority being given to development work and its actual implementation on the ground for which a clean, corruption-free and accountable administration at all levels is an imperative necessity.
- **Respect for rule of law:** Governmental agencies must not be allowed to transgress law even in dealing with critical situations caused by insurgency or terrorism.
- **Countering the subversive activities of terrorists:** Government must give priority to defeating political subversions (e.g. by terrorists and Maoists). The emphasis should be on civil as opposed to military measures to counter terrorism and insurgency.
- **Providing the appropriate legal framework:** The ordinary laws of the land may not be adequate to book a terrorist. This may require special laws and effective enforcement mechanisms, but with sufficient safeguards to prevent its misuse.
- **Building capacity:** The capacity building exercise should extend to the intelligence gathering machinery, security agencies, civil administration and the society at large.

Steps taken by government

- **Enacting legislative framework** such as The Unlawful Activities (Prevention) Act, 1967; The National Security Act, 1980; The Terrorist and Disruptive Activities (Prevention) Act (TADA), 1985 and 1987; Prevention of Terrorism Act, 2002 (POTA)
- **Call for adoption of Comprehensive Convention on International Terrorism (CCIT)**, a proposed treaty which provides a comprehensive global legal framework against terrorism.
- **Cooperation with USA:** In 2011, US-India Homeland Security Dialogue was created, which was the first comprehensive bilateral dialogue on homeland security issues between our two countries.
- **Part of Global Network of Cities on Terror Fight:** Mumbai has now become part of this network formed at UN Level that will exchange techniques and develop infrastructure to combat extremism and strengthen their cyber security system.
- **Countering terrorist financing:** India is part of the Global regime of Financial Action Task Force which aims to counter terrorist financing. For instance, FATF has kept Pakistan in its Grey List for failing to comply with its deadline to prosecute and penalize terrorist financing in the country.

Role of FATF in combating terrorist financing

- **Setting global standards to combat terrorist financing:** FATF ensures all its members have implemented measures to cut off terrorism-related financial flows, in accordance with the **FATF Recommendations**. All members are required to:
 - Criminalise the financing of individual terrorists and terrorist organisations.
 - Freeze terrorist assets without delay and implement ongoing prohibitions.
- **Evaluating countries' ability to prevent, detect, investigate and prosecute the financing of terrorism:** FATF issues two lists namely-
 - **Black list** (officially known as High-Risk Jurisdictions subject to a Call for Action)
 - ✓ The current FATF blacklist includes two countries: **North Korea and Iran**.
 - **Grey list** (officially referred to as Jurisdictions Under Increased Monitoring)
- **Assisting jurisdictions in implementing financial provisions of the United Nations Security Council resolutions on terrorism:** The FATF has developed a range of tools and guidance to help detect, disrupt, punish and prevent terrorist financing.

4.1. ANTI-TERROR LAWS IN THE COUNTRY

Why in news?

Recently, the President gave his assent to the Gujarat Control of Terrorism and Organised Crime (GCTOC) Bill.

Need of Anti-terror legislations

- **Complete the anti-terror infrastructure-** which includes three main elements
 - A law governing all aspects of terrorism
 - A **single investigative agency** to single-minded pursuit of terrorism cases in a time-bound manner
 - An agency to **collate, analyse and disseminate intelligence inputs** relating to terrorism.
- **Inadequacies of existing acts-** Over the years, as acts of terror became more frequent, intense and geographically widespread, aided and abated by external forces, the inadequacies of the general laws, treating them as law-and-order matters, started getting exposed.
- **Deal with terror effectively-** that could effectively deny operating space and maneuverability to terrorist groups and their support structures that would deter them from executing any acts of terror.
 - **Counter federal gaps-** to ascertain inter-operability of the investigating agencies, which fall under the ambit of State as well as the union governments.
 - **Counter cross border terror-** with special focus on the issue of gathering of evidence located abroad.
- **Bring clarity over various aspects related to terror-** including its definition, acts, evidences and procedures, which can be followed while dealing with terrorism.

Issues with anti-terror legislations

- **Incoherence and Misuse-** The haste in legislating anti-terror laws led to a significant amount of incoherence, without substantial thought being given to the unintended consequences of the **slight tweaks in language**.
 - Various other state laws have been made without studying the misuse and impact of TADA and POTA, thus increasing the suspicion of their misuse.
- **Complexities of Indian federalism-** Various state laws have faced hurdles in getting Presidential assent and similarly, legal attempts to bring a National Counter Terrorism Centre were thwarted by the state governments.
- **Legislative gap between Union laws-** such as there was a long gap of four years (since repeal of POTA in 2004 till the amendments in UAPA in 2008) when India did not have any special federal anti-terror legislation.
- **State specific problems-** such as the presence of underworld and organized crime networks in Maharashtra, Arunachal led to the enactment of legislations against organized crime like MCOCA, APCOCA.

4.1.1. UNLAWFUL ACTIVITIES (PREVENTION) AMENDMENT ACT, 2019

Why in news?

Recently, the **Unlawful Activities (Prevention) Amendment Act, 2019** was passed in the Parliament of India.

Key Amendments in the legislation

- **Expands the scope of terror entities-** Previously the central government may designate an organisation as a terrorist organisation, if it, prepares or commits or participates or promotes or otherwise involved in terrorism.
 - Now the government is empowered to **designate individuals as terrorists** on the same grounds.
- **Approval for seizure of property-** Earlier an investigating officer was required to obtain the prior approval of the Director General of Police to seize properties that may be connected with terrorism.
 - Now, if the investigation is conducted by an officer of the National Investigation Agency (NIA), the approval of the Director General of NIA would be required for seizure of such property.
- **Empowering NIA:** Earlier, the investigation of cases may be conducted by officers of the rank of Deputy Superintendent or Assistant Commissioner of Police or above.

- This Bill additionally empowers the officers of the NIA, of the rank of Inspector or above, to investigate cases.
- **Insertion to schedule of treaties:** There were nine treaties listed in a schedule (like Convention for the Suppression of Terrorist Bombings (1997), and the Convention against Taking of Hostages (1979)) to the Act, according to which the Act defines terrorist acts to include acts committed under those treaties.
 - This Bill adds the **International Convention for Suppression of Acts of Nuclear Terrorism (2005)** to the list.

Need and Benefits of these amendments

- **Increasing threats of terrorism-** especially emanating from the cross border infiltration, which have caused multiple civilian as well as defence casualties in India.
- **Many individuals escaped the radar-** Not designating individuals as terrorists, would give them an opportunity to circumvent the law and they would simply gather under a different name and keep up their terror activities.
- **Delay in the current process-** the law required that NIA take prior permission from the respective state DGP to attach the proceeds of terrorism. This delays the process as often such properties are in different states.
- **Requirement of Human Resources-** By empowering officers with the rank of inspectors and above to investigate, the amendment seeks to solve the human resource crunch in the NIA.

Concerns with the amendment

- **Draconian Provisions-** The Central Government will be having the power to declare an individual as 'terrorist', which potentially dangerous because it will empower officials of Union Ministry to brand any person as a terrorist without following due process.
- **Potential of misuse-** The terms terrorist propaganda, terrorist literature etc. are vague terms having a potential of being misused by the authority.
- **Goes against the judicial prudence-** if a person is labelled as 'terrorists merely on the basis of speech and thought. Rather it should be considered only if such speech gives rise to direct and imminent violence.

Way Forward

- **Safeguards against misuse-** The Act have provisions for **four level scrutiny** before any decision is taken on designation of an individual as a terrorist. Proper legal and concrete evidence has to be there to support this and there will be close scrutiny at every level.
 - The different agencies of state should ensure that **due process of law** is applied while dealing with various cases under this legislation.
- **Need to ensure state of the art training-** of young officials as to make them competent in tackling complex cases.
- **Need for a central agency for overseeing evidence collection-** so as to aid investigation process, especially when cases need to connect dots across the borders.
- The primary duty of the state is to **secure the lives and property** of its citizens and this amendment empowers the state in doing so.

4.1.2. NIA (AMENDMENT) ACT, 2019

Why in news?

The Parliament recently passed the **National Investigation Agency (Amendment) Act 2019**, which seeks to expand the powers and jurisdiction of the NIA.

Key Amendments

- **Enhances the scope of Offences:** which are mentioned in the schedule to the Act, such as the Atomic Energy Act, 1962, and the Unlawful Activities Prevention Act, 1967.
 - This amendment enhances this scope to include other offences like human trafficking; offences related to counterfeit currency or bank notes; manufacture or sale of prohibited arms; cyber-terrorism; offences under the Explosive Substances Act, 1908.

- **Enhances the jurisdiction of the NIA:** as the officers of the NIA will have the power to investigate scheduled offences committed outside India, subject to international treaties and domestic laws of other countries.
 - The Union government may direct the NIA to investigate such cases, as if the offence has been committed in India.
 - The Special Court in New Delhi will have jurisdiction over these cases.
- **Additional Provisions for Special Courts:** The NIA Act allowed the central government to constitute Special Courts for the trial of scheduled offences.
 - Now the central government may designate **Sessions Courts as Special Courts** for the trial of scheduled offences, but in consultation with the Chief Justice of the High Court under which the Sessions Court is functioning.
 - When more than one Special Court has been designated for any area, the senior-most judge will distribute cases among the courts.
 - Further, state governments may also designate Sessions Courts as Special Courts for the trial of scheduled offences.

Arguments in favour of this amendment

- **Increase in terror attacks-** after the Prevention of Terrorism Act (POTA) was repealed and with these lacunae in the NIA act, the agencies were inadequately armed to deal with such activities.
- **Presence of ambiguity weakened the case-** So far, the NIA could apply the sections to an accused only if the principal offence is part of its Schedule. Now, it can prosecute people in standalone cases under these Acts. For example, a person being prosecuted under UAPA could be slapped with Arms Act sections, but the NIA so far could not prosecute him under the Arms Act alone.
- **Presence of such powers with all major agencies-** of the world such as the **FBI** of the US. It was able to prosecute David Coleman Headley in the 26/11 attacks because they had powers to register a case in a terror attack that had happened in a foreign country.
 - On the other hand, this lacuna was a reason why the case against the Italian Marines who had shot dead an Indian fisherman off the coast of Kerala in 2012 was not investigated properly. The offence had taken place in international waters, and thus NIA had no jurisdiction
- **Help in faster adjudication-** Earlier, setting up special courts in any state would take six to nine months since a proposal had to be made, High Courts' concurrence had to be obtained, a judge had to be nominated, and a court had to be set up. With existing sessions courts allowed to function as special courts, trial can start immediately.

Arguments against this amendment

- **Potential of Misuse-** several opposition leaders criticised the bill and accused the government of using investigating agencies for "**political vendetta**". Some MPs said the anti-terror law is misused at times to target members of a particular community.
- **Judiciary is already overburdened-** and by designating the session's courts as special courts, it would take away its attention from usual business of the courts.

Way Forward

The functioning of NIA should not depend on political mandate, but on rule of law. It must be ensured that human rights are secured.

4.2. "LONE WOLF" ATTACKS

Why in News?

Recently, a lone wolf attack was carried out by an individual in London.

About Lone wolf Attacks

- These attacks involve threat or use of violence by a **single perpetrator** (or a small cell).
- A lone wolf acts **without any direct support** of any other group or other individual in the **planning, preparation** and **execution** of the attack.

- Though lone wolf prefers to act totally alone, his or her radicalization to action maybe spurred by violent media images, incendiary books, manifestos, and fatwas.
- Ranging from threatening and intimidating people to **indiscriminate shootings, vehicle ramming, stabbing and suicide bombings**, lone wolf terror attacks have become a grave threat.
- Long-term data reveals the proportion of lone wolf attacks, has risen from under five per cent in the mid-1970s to above 70 per cent for the period between 2014 and 2018.
 - U.K. itself has seen 3 major incidents involving knife attacks since November, 2019.

Reasons for recent increase in Lone wolf attacks

- **Ease of radicalization through technology:** Number of online forums and social media profiles, where hate-speech and pro-terrorist sentiment flourishes, has increased. They act as source of inspiration and aid to forge connections to like-minded extremists.
- **Mental illness:** According to some estimates, more than 40 percent of attacks were perpetrated by people with diagnosed mental illness.
- **Increasing extreme ideological movement:** Extreme ideological movements are growing stronger in several European countries. Agitators have exploited the fear of religious minorities and refugees in order to undermine public confidence in government and turn them against the society.
- **Ease of execution:** Terrorist organisations have embraced this tactic to spread violence in countries where coordinated big attacks are difficult to execute due to stringent security.
- **Lax Gun Control regime:** favors lone wolves in carrying out attacks with mass casualties.

Threats associated with Lone Wolf Attacks

- **Hard to detect and prevent:** The tools of intelligence agencies and law enforcement, including undercover sources and intercepted communications, are much less effective against an individual who is not communicating his plans and intentions to others.
- **Hurdles in Profiling:** Lone wolf terrorists comprise a wide variety of violent extremists. Among them are religious zealots, environmental, animal rights extremists etc. Even at the level of the ideological or religious background there is much variety. This makes it harder to counter them at ideological level.
- **Hard to distinguish from internet banter:** It is extremely difficult to differentiate between those extremists who intend to commit attacks and those who simply express radical beliefs or issue hollow threats.
- **Providing a template to violence-prone misfits who might otherwise not have acted:** People who might not have the means, opportunity, or even desire to actually join a terrorist organization might nevertheless come to see lone-wolf attacks as an appealing way to express their rage and avenge perceived injustice.

Lone Wolf attacks in India

Challenges

- **Weakening position of the IS in Iraq and Syria** reduces chances of a traditional regrouping of the terrorist organisation. Hence, the groups might prefer 'lone wolf' attacks by their members, sympathisers, would-be militants and foreign fighters in India.
- **Possibility of Pakistan using it as a tool to advance its state-sponsored terrorism against India.**
 - By sponsoring a widespread circulation of extremist literature and propaganda across India, both online and offline, Pakistan may resort to influencing the 'lone wolves' to carry out terror attacks in India.
- **High potential damage** of lone wolf attacks due to presence of densely populated areas and illegal networks for obtaining firearms in India.
- **Spread of fake news and misinformation:** Fake news propagated through social media sites crystallise biased narratives and seem to legitimise and reinforce the desire to seek violence against the "other".

Steps taken to prevent it

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

Way forward

- **A multi-pronged approach towards radicalization** must be adopted by the government and the security agencies, anchored in human intelligence, strong ties with communities and community leaders and deradicalization programmes.
- **Monitoring social media** can help officials spot potential attackers without previous connections to other terrorists.
- **Try to make lone-wolf attacks less lethal** by limiting access to explosive materials, semiautomatic weapons etc.
- **Focus on gathering intelligence, arresting suspected cell leaders, and destroying terrorist command centers** involved in radicalization activities.
- **Proactive measures** such as training and equipping the local police, contingency plans by the intelligence and counter-terrorism structures, and a robust national counter-terrorism doctrine addressing the different nuances of terrorism are strategically important to subdue any attempts of lone wolf terrorism.
- **Big data analytics** can be used to discern the level of radicalization of potential recruits, their networks and sources of information, funding and leadership in order to help unravel the roots of radicalization.

ENGLISH Medium | 10 Nov 5 PM **हिन्दी माध्यम | 11 Nov 5 PM**

📖 Specific content targeted towards Mains exam

📖 Complete coverage of The Hindu, Indian Express, PIB, Economic Times, Yojana, Economic Survey, Budget, India Year Book, RSTV, etc

📖 Doubt clearing sessions and mentoring

📖 Support sessions by faculty on topics like test taking strategy and stress management.

📖 **LIVE** and **ONLINE** recorded classes for anytime any where access by students.

MAINS 365
One year Current Affairs in 60 hours

JANUARY, FEBRUARY, MARCH, APRIL, MAY, JUNE, JULY, AUGUST, SEPTEMBER, OCTOBER, NOVEMBER, DECEMBER

5. INSURGENCY IN THE NORTHEAST

Introduction

India's state formation process has involved a number of ethnic secessionist insurgencies in several peripheral north-eastern states of Nagaland, Mizoram, Manipur, Assam, Tripura and Meghalaya.

Conflicts in the region can be broadly grouped under the following reasons:

- **Nationality:** Involving concept of a distinct 'homeland' as a separate nation and pursuit of the realisation of that goal by its votaries.
- **Ethnic reasons:** Involving assertion of numerically smaller and less dominant tribal groups against the political and cultural hold of the dominant tribal group. In Assam, this also takes the form of tension between local and migrant communities.
- **Sub-regional reasons:** Involving movements which ask for recognition of sub-regional aspirations and often come in direct conflict with the State Governments or even the autonomous Councils.
- **Developmental issues:** Poverty, unemployment, lack of connectivity, inadequate health care and educational facilities, feelings of neglect and non-participation in governing their own affairs have contributed to the insurgency in the region.



What are the challenges in handling insurgency in the Northeast?

- **Dual responsibility:** For ex- Assam Rifles the country's oldest paramilitary force provides dual service of guarding the porous Indo-Myanmar border and counter insurgency operations
- **Guarding open border** where a free movement regime is also in place for uninterrupted travel to each other's territories by people of both the countries.
- **Taking care of diplomatic sensitivities** as Myanmar, Bhutan etc. are friendly countries.
- **External Support by other nation state:** For eg- alleged arms smuggling by China in North east.
- **Multiplicity of bodies and agencies** like the NEC, DoNER and the recently created North East Forum. There is a need for clarity on the roles between these bodies
- **Other issues:** Delay in project implementation, shortage of funds.

What are the steps taken by the government for the region as a whole?

- **Constitutional protection in Sixth Schedule** which protected not only the tribal laws, customs and land rights; but also gave sufficient autonomy to the tribes to administer themselves with minimum outside interference.
- **Protected Area Permit:** Due to security reasons, certain areas have been declared as Protected Area/Restricted Areas where no foreigner can enter or stay without obtaining permit from the competent authorities
- **Act east policy** to enhance economic cooperation with South East Asian countries will benefit North East.
- **Infrastructural development**
 - **Kaladan Multimodal project** to provide connectivity of North East with rest of India through Mizoram.
 - **Trilateral highway** (moreh (manipur) -mandalay - thailand) will facilitate north east trade with South east Asia.
 - **North-East Road Sector Development Scheme (NERSDS)** is a region-based road development programme in India.

What more can be done?

- **NEC as forum:** The North Eastern council (NEC), having the Governors and Chief Ministers of the North Eastern states as its members, can provide a common forum for discussing security aspects in a comprehensive manner.

- **Multi-stakeholder approach:** A wider representation not just of civil society, scholars and others, but also of professionals is required at any forum addressing the concerns in the North-East.
- **Understanding emotional and psychological aspects of the problems of the different states of the North-East:** Any meaningful policy for the North-East should address the specifics of each state and region.
- **Economic development:** Opening up of economy of this region may be expedited making way for new investments, acquiring of productive assets, reaching potential in tourism etc.
- **Tackling illegal immigration from neighbouring countries:** Identity cards and work permits for those who come for work should be made mandatory.
- **Stress on Dialogue** as an ongoing process to reach concrete solutions by involving all the stakeholders and not a single group.

5.1. NAGA PEACE TALKS

Why in News?

The deadline set by the Union government to conclude the **Naga peace talks ended on a somewhat ambiguous note.**

More about news

- The deadlock between the government and the National Socialist Council of Nagalim (Isak-Muivah) (NSCN (IM)) over a **separate Naga flag and constitution** were the issues holding up a final agreement.
 - Now, NSCN (IM) agreed to a settlement **without a Constitution and with a conditional flag** that can only be used for **non-governmental purposes.**
- Further, it was clarified that before any settlement is arrived at with Naga groups, **all stakeholders including States of Assam, Manipur and Arunachal Pradesh will be duly consulted** and their concerns will be taken into consideration.

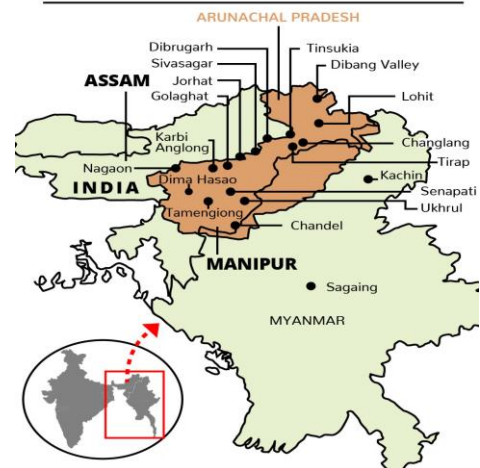
Timeline of Naga conflict and peace talks

- **1946:** Formation of **Naga National Council (NNC)**, under the leadership of **Angami Zapu Phizo**, which declared Nagaland an independent state on August 14, 1947.
- **1952:** Phizo formed the underground **Naga Federal Government (NFG) and the Naga Federal Army (NFA).**
- **1958:** The Government of India **sent in the Army to crush the insurgency and enacted the Armed Forces (Special Powers) Act.**
- **1975:** A section of NNC leaders signed the **Shillong Accord**, under which this section of NNC and NFG agreed to give up arms.
- **1980:** A group of about 140 members led by Thuingaleng Muivah, who were at that time in China, refused to accept the Shillong Accord, and **formed the National Socialist Council of Nagaland in 1980.**
- **1988:** the NSCN split into NSCN (Isak-Muivah)/(IM) and NSCN (Khaplang)/(K).
- **1997:** Government of India signed a **ceasefire agreement with NSCN (IM)**, after 80 rounds of talks.
- **2015:** NSCN-IM, **gave up the idea of Naga sovereignty and “agreed for a settlement within the Indian federation”.**
- **NSCN (IM) demand:** A “Greater Nagalim” comprising “all contiguous Naga-inhabited areas”, along with Nagaland. That included several districts of Assam, Arunachal and Manipur, as also a large tract of Myanmar.
- **NSCN (K) is opposed to the talks**, continues violent methods, though Khaplang died in 2017, weakening it.

Roadblock to Naga Peace talks

- **Nature of demand:** It is considered that the flag and constitution issue is integral to the core issues of the process and, therefore, a final settlement cannot be reached without these.
 - This requires **fundamental changes in the country's federal dynamics.**
- **Existence of Article 371A:** An **amendment to this Article is critical to the ongoing Naga peace process** in order to resolve another substantive issue of settling the question whether Nagas have the right over land and resources, both above and beneath it.
- **Integrity of other states:** None of the three states i.e., Manipur, Assam and Arunachal Pradesh would allow their territories to become a part of the ‘Greater Nagalim’.

‘GREATER NAGALIM’, AS THE NSCN (IM) ORIGINALLY SOUGHT



- For example, in **Manipur, Meiteis** (form a majority in the Imphal Valley) and the Nagas and Kukis, dominate the tribal districts of the hills. For decades, the communities have made **competing demands for ethnic homelands**.
- **Similar demand from other groups:** Political instability has undermined the role of democracy in the state and has fueled apprehensions leading to separate agendas and demands by various factions and organizations. For instance, the **Kuki groups**, also in talks with the government, fear the Naga solution would **carve up their imagined homeland**.

The situation and the negotiations get further complicated due to **continued violence in the region, continuance of Armed Forces (Special Powers) Act** and **People losing faith** in the overall management of the conflict.

Way forward

- Government should **address the confusion due to many interpretations** to “special arrangement” implied in the 2015 agreement, particularly on how the shared sovereignty will be exercised.
- The government should not rush into a solution by declaring deadlines. It should **involve all stakeholders from within and outside the state of Nagaland**, and work towards a solution through a peaceful dialogue process that satisfies all.
- **Other sections’ sensitivities** also will have to be kept in mind. **For example, Kukis**, a tribe engaged in tussle with the Nagas in the Manipur hills, have to be politically assuaged.
 - For instance, recently, the **Naga National Political Groups (NNPGs) and Kuki National Organisation (KNO)** have signed a joint declaration to work together, as they used to separately negotiate political settlements with the Union of India.
- Arunachal Pradesh, Assam and Manipur are wary of the NSCN-IM’s concept of Nagalim that could lead to a redrawing of their boundaries. The government and the NSCN (IM) must be completely **transparent** in their approach and must take into **confidence all genuine political formations, civil society and ethnic groups**.
- **People-to-people contacts** need to be built up so that real problems of the people can be voiced on a larger platform. There is a need for **more cross-cultural openness**, not only between mainstream India and the Northeast, but among the north-eastern states as well.

5.2. THE BODOLAND DISPUTE

Why in news?

Union Ministry of Home Affairs (MHA) has extended ban on the National Democratic Front of Bodoland (NDFB) by five more years, under provisions of **Unlawful Activities (Prevention) Act, 1967**.

More on the news

- NDFB is an **ethnic insurgent organization** demanding an **independent state for the Bodo ethnic group in Assam, formed in 1986**.
- It shares close ties with the **United Liberation Front of Assam (ULFA)**.
- According to the MHA, NDFB poses a threat to the sovereignty and territorial integrity of India and has been involved in illegal and violent activities like extortion, terrorism, obtaining assistance from anti-India forces, ethnic killing, secessionist activities etc.

About Bodoland

- It is a state demanded by a **tribal community called Bodos** in Assam, who comprise of 5%-6% of the state’s population.
- It consists of regions located extreme north of north bank of Brahmaputra river in the state of Assam, by the foothills of Bhutan and Arunachal Pradesh.



Bodoland Territorial Council (BTC)

- It has legislative, administrative, executive and financial powers over 40 policy areas in the **Bodoland Territorial Area District (BTAD)**.
- **BTAD** comprises four districts (**Kokrajhar, Baksa, Chirang and Udalguri**) of Assam.
- It functions under the provision of the **Sixth Schedule of the Constitution** of India.

Timeline of the Bodoland dispute

- **1960s and 1970s** - There were calls from Bodos and other tribes for a separate state of 'Udayachal' as immigrants were accused of illegally encroaching on Bodo-inhabited lands. Demand was raised under the banner of the **Plains Tribals Council of Assam (PTCA)**, a political outfit.
- **1993** - The **Bodoland Autonomous Council (BAC)** was constituted after the Centre, the Assam government and the All Bodo Students Union (ABSU) signed a **tripartite agreement**. However, BAC failed due to non-implementation of various provisions of the Accord.
- **2003** - The **Bodoland Territorial Council (BTC)** was formed after the Centre, the Assam government and the BLT sign a tripartite agreement. The BLT is disbanded.
- **2005** - NDFB agreed to a ceasefire with the Assam government and the Centre. After the treaty was signed, the group splits into three factions. One of those factions, the NDFB (S) continued to carry out violent attacks.
- **2020** - The **3rd Bodo Peace Accord** as tripartite agreement between the **Centre, Assam Government and the banned Assam-based insurgent group National Democratic Front of Bodoland (NDFB) was signed** on 27th January 2020, for bringing a lasting peace in Bodo-dominated areas in Assam.

Key elements of the Bodo Peace Accord

- **Ensuring peace and harmony in the BTAD:** Over 1,615 cadres of different factions of the NDFB surrendered their arms and joined the mainstream within two days of the signing of the agreement.
- **Soothing the sentiments of the Bodos:** The BTAD, will now be known as **Bodoland Territorial Region**. The changed nuance from districts to region is significant as it acknowledges a **Bodo homeland within the state of Assam**.
- **Balancing the aspirations of all:** The new Accord has decided to **demarcate the border** of the Bodoland Territorial Area (BTR). **This is expected to address the issues of both tribal currently outside** the Bodo Council as well as non-tribal currently living within the Council.
- **Strengthening the BTC:** Accord has provided more **legislative, executive, administrative and financial powers** to BTC and amendment to the Sixth Schedule of the Constitution.
- **Protection of Bodo culture and welfare measures:** **The accord has provided for setting up of a Bodo-Kachari Welfare Council** for 'development' of Bodo villages located **outside** the Bodo Council area and declaring Bodo language in Devnagri script as an associate official language of Assam.

Reasons for the demand of independent State

- **Massive Illegal Immigration from Bangladesh:** It has led to certain concerns among the Bodos-
 - **Changing Demography:** It might turn them into a minority in their own land.
 - **Inclusion of illegal migrants in the voters list:** It is viewed as a deliberate ploy to empower an outside group, so that the Bodos lose their political power.
- **Threat of loss of distinct language and culture:** Due to forced assimilation.
- **Growing Unease:** Due to the political empowerment of the minority communities in the BTAD in recent years.
- **Failure of The Bodo Territorial Council (BTC):** Weak administrative institutions and divisive politics of the members of the BTC have also added to their insecurity.

Way Ahead

- The government should **strengthen the autonomous, administrative** divisions in Assam established on the basis of the Sixth Schedule of the Constitution.
- Establish a **land record system** that is computerised and accessible to the local people, and which can address the fear of loss of land to the outsiders.
- **Improve** the presence of both the **state civil administration and the law enforcement agencies** in areas that are identified as highly susceptible to ethnic violence.
- The government should take measures to **improve the other economic sectors** of the region like development of agro-based industries, tourism and hydroelectricity etc.
- **Measures** to protect their **language and cultural identity** should be taken.

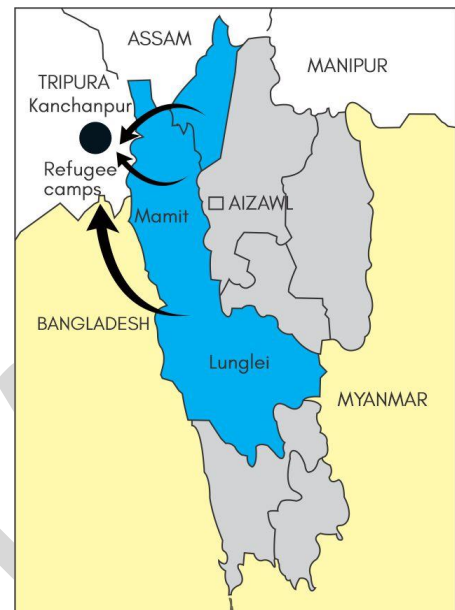
5.3. BRU REFUGEE CRISIS

Why in news?

A four-party agreement among the Centre, Mizoram government, Tripura government, and leaders of Bru community was signed to end the 23-year old Bru-Reang refugee crisis.

About the Crises

- The Bru community, also referred to as Reangs, resides in Mizoram, Tripura, and parts of southern Assam, and is ethnically distinct from the Mizos of Mizoram.
- There are over 40,000 Brus living in four districts of Mizoram. At present, over 30,000 Brus are living in the refugee camps in Tripura after they fled Mizoram following ethnic clashes with the Mizo tribes in 1997.
- The **first signs of conflict** between the two communities emerged in 1995 when Mizo organizations - the Young Mizo Association and the Mizo Students' Association - **demand that Brus be left out of the Mizoram's electoral rolls** as they were not an indigenous tribe.
- The Brus retaliated by forming an armed organization, Bru National Liberation Front, and a political body, Bru National Union. The two demanded more political autonomy for Mizoram's Brus and a **Bru Autonomous District Council (ADC) under the Sixth Schedule** of the Constitution.
- In 1997, following ethnic tension over an incident in Mizoram, **around 5,000 families comprising over 30,000 Bru tribals were forced to flee the state and seek shelter in Tripura.**



Efforts made by the Union Government

- **Since 2010**, the Union government has been assisting the two State governments for taking care of the refugees. Till 2014, 1622 Bru-Reang families returned to Mizoram in different batches.
- In 2018, **an agreement was signed between the Union government, the two State governments and representatives of Bru-Reang refugees**, as a result of which the aid given to these families was increased substantially.
- Subsequently, 328 families comprising of 1369 individuals returned to Mizoram under the agreement. But there had been a **sustained demand of most Bru-Reang families that they may be allowed to settle down in Tripura**, considering their apprehensions about their security.

Key features of present pact

- Around **34,000 Internally Displaced Brus will be settled in Tripura** and would be given aid from the Centre to help with their rehabilitation and all-round development, through a **package of around Rs 600 crores.**
- These people would **get all the rights** that normal residents of the States get, and they would now be able to enjoy the **benefits of social welfare schemes** of Centre and State governments.
 - The Bru refugees in Tripura will be given aid for their rehabilitation and would be given the **tribal status** and included in the **voter list of the state.**

Persistent Challenges

- It is **doubtful** whether the land that is allocated to **Brus in Tripura will be accepted by the domicile tribes in Tripura.**
- Till the pact, the Tripura Government was eager to repatriate the Brus to Mizoram. As the new pact settles the Brus in Tripura, it needs a **lot of political will from Tripura to implement welfare programmes for the Brus.**
- The **existing Bru families in Mizoram are still opposed by some ethnic organizations of Mizoram**, which might trigger another exodus if there is no settlement at the place of the conflict.

Conclusion

The pact is hailed as a settlement for the **over two-decade old ethnic disturbances** between the tribes of the North East and consistent approach towards a peaceful North-East India. This also provides a **model on how to deal with Internally Displaced Persons (IDPs).**

6. POLICE MODERNIZATION

Introduction

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

Issues in functioning of the Police Forces

- **Overburdened police force:** The actual strength of police force in averages around 137 per lakh people, which is against the sanctioned strength and United Nation recommend strength of 181 police per lakh and 222 police per lakh people respectively.
- **Quality of investigation:** The poor quality of investigation of crime lead to only 47 % conviction rate for crimes (The Law Commission 2012). The police lack training and expertise required to conduct professional investigations. They also have insufficient legal knowledge and inadequate forensic and cyber infrastructure.
- **Police accountability:** Control over police by political executive has to lead to abuse of police personnel, its criminalisation and interference with their decision-making authority. In this effect Supreme Court in Prakash Singh case issued guidelines.
- **Boost personnel capacity:** Majority of police personnel comprises of constabulary rank (86%), with low and inadequate training which leads to mismanagement of law-and-order situation. The high stress levels, erratic working hours, family issues or the thankless nature of the job are some of the reasons for suicide and fight with colleagues amongst policeman.
- **Lack of infrastructure**
 - There were considerable delays in procuring new infrastructure like vehicles.
 - **Basic facilities like Forensic labs and Fingerprint bureaus** are still in shortage.
 - **The training academies** in most of the states have very poor infrastructure and Police training to use modernized equipment and processes was low.
- **Police Public Relation**

The perception of police among the people is of trouble creator rather than trouble shooter. One the way to address these challenges is through the community policing model. Various states have implemented the programme like 'Janamaithri Suraksha Project' of Kerala, 'Joint Patrolling Committees' of Rajasthan, Assam through 'Meira Paibi', Maharashtra through 'Mohalla Committees'.

Several efforts towards Police Modernization have been made by the Government. These include **National Police Commission 1977-81**, **Ribeiro Committee 1988**, **Padmanabhaiah Committee 2000**, **Malimath Committee 2002-03**, **Supreme Court Decision on Prakash Singh vs Union of India 2006** and **Police Act Drafting Committee II 2015**.

Guidelines issued in Prakash Singh Case

- Establishment of **three institutions for police organization**:
 1. a **State Security Commission (SSC)** to prevent unwarranted influence or pressure on the police by state government.
 2. a **Police Establishment Board (PEB)** to decide transfers, postings, promotions and other service-related matters of police officers.
 3. a **Police Complaints Authority (PCA)** to inquire into public complaints against police officers regarding serious misconduct.
 4. a **National Security Commission (NSC)** at the union level to prepare a panel for selection and placement of Chiefs of the **Central Police Organisations (CPO)**
- **Director General of Police (DGP) should be selected from three senior-most officers** of the state empaneled by the Union Public Service Commission and must have a minimum two-year tenure.
- Officers in key positions in the field (Inspector General in charge of Range, Station House Officer) must be **given a two-year tenure**.
- In order to improve the quality of investigation, the **investigating police must be separated from law-and-order police**.

Recent initiatives towards Police Reforms

- **Modernization of Police Forces Scheme:** The scheme focuses on strengthening police infrastructure by construction of secure police stations, training centres, police housing (residential) and equipping police stations with required mobility, modern weaponry, communication equipment and forensic set-up etc.
- **Administrative changes:** On the administrative side, changes include **separation of investigation from law and order, specialized wings** for Social and Cyber Crimes are initiated in several states.
- **Technological reforms:** Various technological reforms are pushed including modernization of the control room, fast tracking **Crime and Criminal Tracking Network and System (CCTNS)** and pushing for incorporation of new technology into policing.
- **Moving towards Commissionerate System wherever appropriate:** Recently, Uttar Pradesh cabinet approved implementation of the commissioner system of policing for the two cities, **Lucknow and Noida**, that will give magisterial powers to their top police officers.

Dual system	Commissionerate system
Dual command structure over the district police means that control and direction over the police vests with the SP (head of district police) and the District Magistrate (executive).	Unified command structure with the Commissioner of Police (rank of the Deputy Inspector General or above) as the sole head of the force within the city.
Separation of powers of the DM (e.g., issues arrest warrants and licenses) and the police (e.g., investigate crimes and make arrests). Therefore, less concentration of power in the police, and accountability to DM at the district level.	Powers of policing and magistracy concentrated in Commissioner. Directly accountable to state government and state police chief. Lesser accountability to the local administration. <ul style="list-style-type: none"> • It gives an integrated command structure which helps in speedy decision. • It reduces workload of District Magistrate

- **National Intelligence Grid (NATGRID):** NATGRID, an attached office of Ministry of Home Affairs (MHA), is the integrated intelligence grid which connects databases of core security agencies. It was **proposed after the 2008 Mumbai terror attacks.**
 - NATGRID is very effective in **communication and gathering of information**, to keep **all data on previous intelligence alerts**, providing **real time actionable intelligence** and **respond to evolving threats like radicalization through Social Media.**

Smart Policing <ul style="list-style-type: none"> • The concept of SMART Policing was articulated by Prime Minister in the DGP / IGP Conference 2014 held at Guwahati. • Broadly, smart policing involves interventions incorporating application of evidence-based and data-driven policing practices, strategies and tactics in order to prevent and control crime. • Benefits of SMART Policing <ul style="list-style-type: none"> ○ It promotes pro-active policing by preventing criminal activity through enhanced police visibility and public engagement. ○ Smart policing encourages a system-wide and strategic view of police operations. ○ It encourages focus on outcomes i.e. reduced crime & safer communities in cost effective ways. ○ Smart policing paradigm promotes integration & interoperability of information & communication systems. ○ These initiatives help to protect civil rights and to make police force more citizen friendly. 	'SMART' S - Strict and Sensitive M - Modern and Mobile A - Alert and Accountable R - Reliable and Responsive T - Techno-savvy and Trained
--	---

6.1. POLICE PREPAREDNESS DURING COVID-19 PANDEMIC

Why in News?

The ongoing health crisis due to COVID-19, coupled with the nationwide lockdown and economic hardships, has created a unique law and order challenge. So, Police which is one of the frontline responders to the pandemic often has to go beyond its call of duty.

Changing role of Police amid the pandemic

Generally, Police is seen as a State entity that enjoys power to uphold Personal security and Community security. However, this pandemic has strengthened and accelerated the need of Police to get involved into other aspects of Human security as well i.e. Economic security, Food and Health security and Environmental security (hygiene). More specifically, key areas of police role during pandemic are highlighted as follows:

- **Monitoring and Enforcement:**
 - **Providing temporary quarantine and enforcing home quarantine, social distancing.** For Ex. Kasaragode Police followed 'triple-lock' strategy in which police used traditional methods like barricades to restrict movement, human surveillance and app-based tracing and delivery of essentials and medicines.
 - Capacities nurtured over the years like Call Detail Records (CDR Analysis) of the mobile phones of the affected people, along with other cyber forensic tools have been used by the police to trace the contacts from affected persons.
- **Public Awareness:** Spreading information through various platforms like social media, speakers and dispelling misinformation. Ex: road paintings or coronavirus shaped helmets were used to spread awareness and to show the importance of hygiene.
- **Supply chain management:** Issuing e-passes to allow smooth movement of supplies and using police control room (PCR) vans to facilitate last-mile delivery.
- **Migrants:**
 - Support local authorities in transport of stranded migrant workers to community spaces, government schools set up as temporary shelters.
 - Distribution of food, disinfecting transportation vehicles, ensuring social distancing at stations etc.
- **Reopening industries:**
 - Facilitate resumption of all kinds of work like construction, agriculture or manufacturing.
 - Support local authorities in conducting spot checks at work sites and enlist the support of Reserve Forces, Home Guards, National Cadet Corps, and other defence or policing forces to manage social distancing and hygiene when work resumes at sites.
- **Police Health:** Keeping older personnel away from frontline, plan for rotational shifts, maintaining quarantines for sick personnel and procuring and maintaining Personal Protective Equipment (PPE) in adequate quantities, including masks, gloves, hand sanitiser.
- **Organisation Structure:**
 - **Nodal Authority:** Have adequate teams in 24x7 shifts, Coordinate with other departments, Use geographic information system for better visualisation etc.
 - **Internal communication:** Conduct briefing and debriefing sessions, using recorded messages and regularly informing frontline officers about the latest orders and implementation thereof.
- **Proactive Community Policing:**
 - Coordinate with resident welfare associations and panchayats
 - Protect senior citizens by providing information and enabling services and groceries to the doorstep
- **Crimes:**
 - Keep some personnel available for regular crime prevention and investigation duties and respond to changing nature and intensity of crime. Ex. Domestic violence cases have increased during lockdown.
 - Active monitoring of social media through Cyber Crime Cell and Launch citizen-based campaign to report and deter cyber-crimes, including rumour mongering, cyberbullying, hate speech and fake news.
- **Prisons and Juvenile homes:** Monitor and prevent outbreaks among the detained population and inculcate hygiene and social distancing practises. Make arrangement for video calls with lawyers. Release select prisoners/undertrials on parole or bail. Reduce detention for minor crimes.

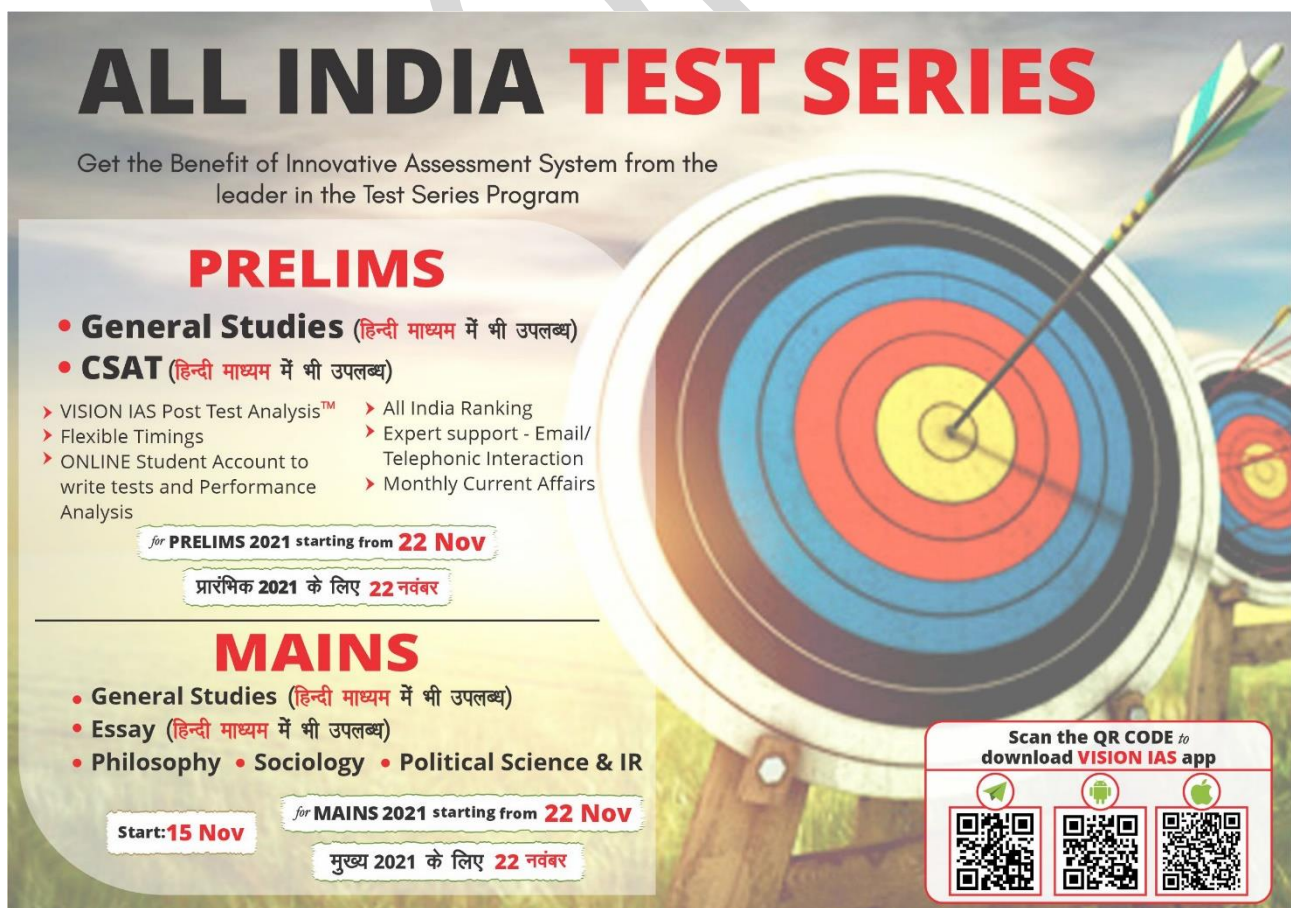
Challenges faced in fulfilling their roles

- **Staffing:** If there is large-scale spread of the virus amongst members of the force or in their families, there could be significant drops in the available fighting strength of the force, which is already well below desirable levels
- **Ill-equipped**
 - They are out with **nil or little protective gear** — they wear the same substandard masks for days.
 - **Infrastructure on ground**, particularly police response vehicles are not fabricated with the necessary equipment to handle emergencies.
- **Ill-trained**
 - Over the last five years, on an average, **only 6.4% of the police force have been provided in-service training**, the SPIR found. Considering the additional protocols and risks involved in responding to a pandemic, this training falls grossly inadequate.

- Police are trained to be rough and **necessary soft skills** to gain public confidence and respond to victims of trauma **are largely missing**.
- **Pervasive public refusal to adhere to the rules and regulations** is making their task even more difficult.
- **A standard operating procedure is absent** in various police departments on how to respond to various issues related to pandemic. For ex: there was much confusion regarding disposal and handling of dead bodies because of COVID-19.

Way Forward

- **Finance:** Seek funds via corporate social responsibility route through a special purpose vehicle with independent oversight to cover for any shortfalls in funding of Police.
- **Domestic and gender violence and child abuse:** Build local intelligence network to get alerts on such cases, ensuring active response on helpline numbers and coordinate with NGOs and medical and rehabilitation centres with and counselling support are needed.
- **Addressing Police high-handedness:** this aberration needs further professional standard settings, behavioural and ethical norm mainstreaming and training inputs.
- **Gaining public trust:** pandemic has strengthened the need for more collaborative ways of working and partnerships within and across the public and private sectors, moving towards a more inclusive approach that embeds societal responsibility.



ALL INDIA TEST SERIES

Get the Benefit of Innovative Assessment System from the leader in the Test Series Program

PRELIMS

- **General Studies** (हिन्दी माध्यम में भी उपलब्ध)
- **CSAT** (हिन्दी माध्यम में भी उपलब्ध)

- VISION IAS Post Test Analysis™
- Flexible Timings
- ONLINE Student Account to write tests and Performance Analysis
- All India Ranking
- Expert support - Email/Telephonic Interaction
- Monthly Current Affairs

for **PRELIMS 2021** starting from **22 Nov**

प्रारंभिक 2021 के लिए **22 नवंबर**

MAINS


- **General Studies** (हिन्दी माध्यम में भी उपलब्ध)
- **Essay** (हिन्दी माध्यम में भी उपलब्ध)
- **Philosophy • Sociology • Political Science & IR**

Start: **15 Nov**

for **MAINS 2021** starting from **22 Nov**

मुख्य 2021 के लिए **22 नवंबर**

Scan the QR CODE to download **VISION IAS** app



7. MILITARY MODERNIZATION

7.1. DEFENCE PRODUCTION

Introduction

India is one of the largest importers of conventional defence equipment and spends about 30% of its total defence budget on capital acquisitions. In the light of this, it becomes important that the focus be shifted towards defence production.

Current Status of Defence Production in India

- India remained the world's **second-largest arms importer** during 2015-19, with Russia as its largest supplier.
 - Although **Russia's share** of the Indian weapons market **has declined from 72% to 56%**.
- Estimates suggest the Indian armed forces **could spend about \$130 billion** to procure defence equipment in the next five years. The share of domestic procurement in overall Defence procurement is about **60 percent**.
- The size of India's defence industry is **estimated to be Rs 80,000 crore**. "While the contribution of the **public sector** is estimated to be **Rs 63,000 crore**, the share of **private sector** has steadily grown to Rs **17,000 crore** over the years.
- **Defence exports:** In 2018-19, they were worth Rs 10,745 crore, a growth of over 700 per cent since 2016-17. India exports to more than 40 countries.
- The defence industry is ably **supported by a strong base of over 8,000 MSMEs** that provide strength and vibrancy to the defence supply chain.

Prevalent challenges in improvement of Defence Production

- **Absence of designing and development capabilities**, resulting in associated lack of design rights and patents in defence technology.
- **Limited participation of the private sector** as seen from the aforesaid data.
- **Lack of industry-academia-defence linkage** leading to a disconnect between industrial capabilities & academic research and defence needs.
- Defence procurement is a **highly specialized activity that requires a prior estimation** of the development and production timelines involved, which is extremely difficult.
- **India's export market is very limited** vis-à-vis the size of its domestic industry.

Role of Private Sector in Defense Production

- As is mentioned above, the role of Private sector is currently very limited in defense production. (**approximately 23% of the total defense production in India.**)
- **Potential benefits with increased participation of private sector:**
 - The government wants to double domestic production in defense and quadruple exports by 2025. This may not be possible without **private sector investment and production capacity**.
 - Involvement of private sector brings with itself **enlarged human resource pool**.
 - Private sector in Defense could provide a **fillip to the overall economy** by **increasing exports, generating more employment** and **creating ancillary industries** around defense production.
 - In the recent past, **the private sector has also shown larger appetite** than public sector in **acquiring foreign companies/production facilities** and **forming joint ventures** with major global defense companies.
- **Prevalent constraints for the participation of Private Sector:**
 - **High risk on returns** and **defense manufacturing base being highly capital and technology intensive** deters private players from entering the markets.
 - This coupled with **long gestation period for investment, irregular flow of orders, rigorous policies/tax systems** together with **lack of economies of scale in production** further discourages private players.
 - Further, the **Government's biased approach towards Public sector entities**, as these have vast infrastructure, nominated order, investments, and technology collaborations at their disposal through Government support; result in a **lack of a level playing field for the private sector**.

7.1.1. DRAFT DEFENCE PRODUCTION AND EXPORT PROMOTION POLICY (DPEPP) 2020

Why in News?

Recently, Ministry of Defence proposed Draft Defence Production and Export Policy 2020 with an aim to double India's defence production in five years.

Need for an effective defence policy

- To develop a **dynamic, robust and competitive Defence industry**, including Aerospace and Naval Shipbuilding industry to cater to the needs of Armed forces with quality products.
- To **reduce dependence on imports** and take forward "Make in India" initiatives through domestic design and development.
- To **promote export of defence products** and become part of the global defence value chains.
- To **create an environment that encourages R&D**, rewards innovation, creates Indian IP ownership and promotes a robust and self-reliant defence industry.

Other initiatives launched alongside the policy

Naval Innovation and Indigenisation Organisation (NIIO)

- The NIIO puts in place **dedicated structures for the end users to interact with academia and industry** towards fostering innovation and indigenisation for self-reliance in defence.
- It was accompanied by a compendium of **Indian Navy's Indigenisation perspective plans** titled 'SWAVLAMBAN'.

SRIJAN

- It is a **'one stop shop online portal that provides access to the vendors** to take up items that can be taken up **for indigenization**.
- There are over 3000 unique items with a value of over Rs 10,000 Crore that are available through the portal.

Key Guidelines announced in the policy

- **Procurement Reforms** include **Project Management Unit** for supporting the acquisition process and facilitate management of the contracts and a **Technology Assessment Cell (TAC)** would make an assessment of the Technology Readiness Level (TRL) levels.
- **Support to MSMEs/Start-ups** for setting up of an **indigenization portal with an industry interface** and creation of a **Defence Investor Cell** in Department of Defence Production.
- **Investment Promotion and Ease of Doing Business** - **Investments would be encouraged** to provide specific focus on certain identified segments and technological areas such as development of **Aero Engines Complex, Maintenance Repair & Overhaul (MRO) and Critical Technologies & Materials**.
- **Innovation and R&D** - **DRDO** in consultation with the Services and in collaboration with other scientific and industrial establishments would **set up missions in select areas to develop futuristic and critical systems/platforms/materials**.
- **Reforms in DPSUs and Ordnance Factories** by increasing **Corporatization of ordnance factories** and projecting DPSUs as **System Integrators in the Defence Ecosystem**.
- **Improving Quality Assurance (QA) and Testing Infrastructure** through **Defence Testing Infrastructure Scheme (DTIS)**.
- **Export Promotion** through efforts like **Export Promotion Cell** set up to promote Defence exports and creation of an **Open General Export License (OGEL) regime**.

Related News

Defence Testing Infrastructure Scheme (DTIS)

- Recently defence minister approved the launch of DTIS with an outlay of Rs 400 crore for **creating testing infrastructure** for defence and aerospace manufacturing.
- **The objective is to promote indigenous Defence Production**, with special focus on participation of MSMEs and Start Ups.
- **The DTIS guidelines specify the establishment of testing facilities for drones and Unmanned Aerial Vehicles (UAVs), radar, electronics/telecom equipment, rubber testing, noise and shock testing, specialised driving tracks, ballistics and blast testing, and environmental test facilities etc.**

7.2. DEFENCE ACQUISITION PROCEDURE, 2020

Why in News?

Recently Defence Ministry unveiled Defence Acquisition Procedure, 2020 (erstwhile Defence Procurement Procedure (DPP)).

More on News

- DAP has been aligned with the **vision of the government's 'Aatmanirbhar Bharat' (self-reliant India) initiative and to empower Indian domestic industry** through 'Make in India' projects with the ultimate aim of turning India into a global manufacturing hub.
- It has come into effect from October 1, 2020 and will **supersede the Defence Procurement Procedure (DPP) of 2016**.
 - The first DPP was promulgated in the year 2002 and has since been revised periodically to provide impetus to the growing domestic industry.
- Earlier in Aug 2019, Defense Ministry had constituted **Committee under Apurva Chandra** for preparation of DAP-2020.

Significance of policy

- **Reduce dependence on imports:** India is one of the top defense hardware purchasers in the world, spending billions of dollars each year according to various estimates.
- **Boost overall economy:** Government aims for a turnover of ₹1.75 lakh crore in defense manufacturing by 2025 with the sector identified as having the potential to boost the overall economy.
- **Improve capabilities of the Armed Forces:** DAP 2020 provides impetus to indigenization and facilitates technology infusion to enhance future capabilities of the Armed Forces.
- **Defined role for Private sector:** Private investment will be a major contributor to the 'Make in India' initiative, accelerate manufacturing-led industrial growth and for capital and technology advancement.
- DAP will **ensure timely acquisition of military equipment, systems and platforms as required by the Armed Forces** in terms of performance, capabilities and quality standards, through optimum utilization of allocated budgetary resources.
- **Complex and unique decision making:** Defense acquisition has certain unique features such as supplier constraints, technological complexity, foreign suppliers, high cost, foreign exchange implications and geo-political ramifications which would be better addressed through a designated policy.
- **Streamlining and simplifying process:** DPP favors **swift decision making, provides for suitable timelines** and delegates powers to the appropriate authorities to ensure an efficient and effective implementation of the procurement process, by all stakeholders concerned.

Key points in policy

- **Offset policy revised:** Government has changed 15-year-old policy by removing the clause for offsets for inter-government agreement (IGA), government-to-government defence deals and single-vendor contracts for the procurement of arms and military platforms for the armed forces.
 - The Under the offset policy, the foreign defence entities were **mandated to spend at least 30% of the total contract value in India** through procurement of components, transfer of technologies or setting up of research and development facilities.
- **Notify a List of Weapons/Platforms for Ban on Import:** This is done to ensure that no equipment as mentioned in the list is procured through import post timelines notified.
- **For Indigenisation of Imported Spares:**
 - **New Category of Buy (Global – Manufacture in India):** It has been incorporated in line with new FDI Policy and to encourage foreign original equipment manufacturers (OEMs) to setup 'manufacturing or maintenance entities' through its subsidiary in India.
 - Recently there was enhancement of **FDI through automatic route from 49% to 74% in defence**.
 - **Request For Information (RFI):** RFI stage will explore willingness of the prospective foreign vendors to progressively undertake manufacture and setup an indigenous ecosystem at the spares/sub component level.
 - **Reservation in Categories for Indian Vendors:** The categories of Buy (Indian-IDDM), Make I, Make II, Production Agency in Design & Development, Ordinance Factory Board/DPSU and SP model will be exclusively reserved for Indian Vendors.
- **For Time Bound Defense Procurement Process, Faster Decision Making and Ease of Doing Business:**
 - **Setting up of project management unit (PMU):** It will facilitate obtaining advisory and consultancy support in specified areas to streamline the acquisition process and support contract management.
 - **Simplification of Trial Procedures:** DAP 2020 emphasizes the need to conduct trials with an objective to nurture competition based on the principles of transparency, fairness and equal opportunities to all and not as a process of elimination.
 - The policy also provides for a **single stage accord of AoN (Acceptance of Necessity)** in all cases up to ₹500 crore to avoid delays in approval of acquisition proposals.

- **Leasing:** It has been introduced as a new category for acquisition in addition to the existing 'Buy' and 'Make' categories to substitute huge initial capital outlays with periodical rental payments.
 - This will be **useful for military equipment not used in actual warfare like transport fleets**, trainers, simulators, among others.
- **Strategic Partnership Model (SPM):** Acquisitions under the Strategic Partnership model refer to participation of private Indian firms along with foreign OEM in 'Make in India' in defense and **play the role of a System Integrator** by building an extensive eco-system comprising development partners, specialized vendors and suppliers, in particular, those from the MSME sector.

Related News

Integrated Air Defence Weapon System (IADWS)

- Recently, US has approved the sale of an **IADWS to India** at an estimated cost of \$1.9 billion.
- **Integrated Air Defence Weapon System (IADWS)**
 - The Integrated Air Defence Weapon System (IADWS) is **called as the National Advanced Surface to Air Missile System (NASAMS-II)**.
 - It will be a **combination of different weapons** like Stinger missiles, gun systems and advanced medium-range air-to-air missiles (AMRAAMs), backed by 3D Sentinel radars, fire-distribution centres and command-and-control units.

7.3. PERMANENT COMMISSION AND COMMAND POSITIONS TO WOMEN ARMY OFFICERS

Why in News?

Supreme Court of India has made a landmark verdict in **The Secretary, Ministry of Defence versus Babita Punia and Others case (2011-2020)**, by **allowing permanent commission (PC) status to women officers in Short Service Commission (SSC)** in the Indian armed forces and making them **eligible for command positions**.

Background

- Women officers have been serving in the Armed Forces for about 80 years. They were inducted in the **Military Nursing Service in 1927** and in the **Medical Officers cadre in 1943**.
- Starting in 1992, other branches like **Army Ordnance Corps, Army Education Corps (AEC) and Judge Advocate General (JAG)** were opened up, followed by opening up of more Arms/Services gradually over the years.
- Initially, they were brought in for 5 years of service under **Women Special Entry Scheme**, which was later converted into **SSC in 2006**. The tenure of engagement was increased to 10 years in 1996 and further extended to 14 years in 2004.
- In 2008, Women became eligible for **PC in Army Education Corps and Judge Advocate General Department**. However, they are still excluded from some Combat arms such as **infantry and armored corps**.
- A case was first filed in Delhi High Court by women officers in 2003. In **2010, Delhi High Court, in a landmark judgement**, had directed the government to allow grant of permanent commission to women serving in short service commission. But the order was never implemented and was challenged in the Supreme Court by the then government.
- After this verdict in 2010, **Navy and the Air Force allowed permanent commission for women** officers in branches like Fighter Pilots and Naval Armament Inspectorate respectively. But the Army stalled.
- Last year, **Ministry of Defence (MoD) decided to grant permanent commission to women in 8 Arms/Services of Indian Army** where they are inducted for Short Service Commission.
- **Major concerns that remained:**
 - **2019 order of the MoD:**

Organization of Indian Army

- Indian Army functions under two parts namely **Combat Arms and Services**.
- **Combat Arms** consist of **(Fully) combat roles** like Armoured corps, infantry and mechanised infantry as well as **Combat Support roles** like Corps of Army Air Defence, Army Aviation Corps, Corps of engineers and Corps of signals.
 - Gorkha Rifles, Dogra regiment, Punjab Regiment etc. come under Infantry.
- **Services** consist of Army Service corps (ration, transport and clerks), Army Medical Corps, Army ordnance corps (armament, ammunition, vehicles, clothing and all equipment), The Intelligence corps etc.
- **Commissioned officers** are the leaders of the army and command anywhere from Platoon, Company, Battalion, Brigade, Division, Corps & the Whole army.

- ✓ it was **only for officers with less than 14 years of service**, thus keeping out those who have served longer, and have been petitioners.
- ✓ it would only keep them in the **staff appointments rather than command position**.
- **Women officers in SSC could not attain a rank of Colonel or above** unlike Permanent Commission Officers.
- **Pension benefits were denied to women officers in SSC** because they get eligible for the same after 20-24 years of service.

About the recent SC verdict

What it allows	What it doesn't allow
<ul style="list-style-type: none"> • All women serving as SSC are now entitled to opt for PC — they are qualified for PC as much as all male SSC officers are entitled to opt for the PC. • Applies to women in all in 10 branches of the SSC Arms/Services of the Army — no exceptions. • It has also made recommendations to correct the anomalies including in the matter of pensions due to women Officers, who have been serving and completed more than 14 years of service. • Those who served 20 or more years, whether or not they got a PC, will be entitled to pension benefits. • Women were already allowed to be Platoon and Company commanders, but never a Unit even if they were in Permanent Commission. The verdict enables them to become Commanding Officers in units and larger groupings which are headed by Colonel and above ranks respectively. • Command is now open to women officers — this doesn't necessarily mean commanding to fight battalions, but that women can rise to the colonel level to be eligible for which 15 years of service is required. A command can also be of a non-fighting unit. 	<ul style="list-style-type: none"> • Does not open combat arms (infantry and armored corps) to women — the judgment leaves it to the government of the day, without nudging in any direction. • Does not make permanent commission mandatory — a woman officer can opt for it, but does not get it mandatorily, or by right. • No such thing as a right to take command of something — command positions are decided on the basis of vacancies, qualifications (academic, performance, medical). It usually takes 20 years for an officer to get to this level. • Does not amount to an affirmative action/reservation of jobs in PC or command position — it promises equality of treatment, but the discretion of granting command and PC posts lies with the Army and government, but the decision must be explained.

Way Forward

India began recruiting women to non-medical positions in the armed forces in 1992, yet they **make up about 4 percent of the army's more than one million personnel**, according to latest data. Moreover, **6.7% of the Navy and 13.28% of the Air Force personnel** were women as of June 2019. So, it suggests that India remains a long way from equal representation in the army and other branches of the military.

- More measures like opening the doors of the **National Defence Academy**, which is still reserved only for boys post-schooling, and **adding women to the rank and file** (in the same way police has woman constables) are also needed to ensure women get the representation they deserve.
- In the navy and air forces, certain combat roles are open to women, but there is no such provision yet in the army. We should **follow the examples of Australia, Germany, Israel and the United States, which allow women to take on combat roles.**
 - Women should get their fair share of respect and honour in army as **30% of the total number of women officers are in fact deputed to conflict areas** which shatters the suppositions that women are weak or unsuitable to perform her duties on rough terrains.

7.3.1. WOMEN IN COMBAT ROLE

Why in news?

The Supreme Court judgement has not pushed for inclusion of women in combat roles indirectly highlighting it as an executive decision.

What are the advantages of opening combat roles for women?

- **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.
- **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.

What are the challenges in effecting the same?

- **Condition in Army:** The field conditions in the Army are much more rugged and proximity to comrades and adversary poses greater challenges.
- **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.

Way forward

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**. 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.

7.4. CHIEF OF DEFENCE STAFF (CDS)

Why in news?

- Recently, Ministry of Defence (MoD) created the post of Chief of Defence Staff (CDS) to provide "effective leadership at the top level" to the three wings of the armed forces.
- The outgoing Army chief, **Gen. Bipin Rawat has been appointed as the country's first Chief of Defence Staff (CDS)**.

Background

- The first proposal for a CDS came from the **Kargil Review Committee (KRC)**, set up in 2000.
- In 2011, the **Naresh Chandra Committee on defence and security** also suggested a watered-down version of the CDS proposal.
- **Shekatkar Committee** which submitted its report in 2016 also opined for CDS, having recommendations pertaining to tri-service integration.

About CDS

- The post of Chief of Defence Staff created in the **rank of a four-star General** with salary and perquisites equivalent to a Service Chief.
- CDS will act as the **principal military adviser** to the defence minister on all tri-services matters. The three Chiefs will continue to advise Defence Minister on matters exclusively concerning their respective Services.
- CDS **will not exercise any military command**, including over the three Service Chiefs, so as to be able to provide impartial advice to the political leadership.
- He will serve as the **permanent chairman of the Chiefs of Staff Committee (CoSC)** which comprises the three service chiefs.
- As the Permanent Chairman of Chiefs of Staff Committee, CDS will perform the following functions:

- CDS will **administer tri-services organisations** including those related to Cyber and Space.
- Be a member of the **Defence Acquisition Council (DAC)** chaired by the Defence Minister and the Defence Planning Committee headed by National Security Advisor
- Function as the **Military Adviser to the Nuclear Command Authority**.
- Implement the **five-year Defence Capital Acquisition Plan (DCAP)** and the two-year roll on **Annual Acquisition Plans** as a follow up of the Integrated Capability Development Plan.

Need for CDS

- **Inadequate existing structure:** India has had a feeble equivalent to CDS, known as the **Chairman, Chiefs of Staff Committee (CoSC)**, where the senior most among the three Service Chiefs is appointed as head.
 - However, the CoSC arrangement has been often cited “unsatisfactory”, and its Chairman as a “figurehead”, therefore could not further tri-service integration, resulting in inefficiency and an expensive duplication of assets.
- **Need for a central nerve Centre:** India currently has 17 Service commands at different locations and duplicating assets, therefore the CDS is seen to be **vital to the creation of “theatre commands”** as well as integrating tri-service assets and personnel.
- **To weed out the policy paralysis:** Major deficiency of the planning process led to lack of inter- and intra-service prioritization, duplication of efforts, and sub-optimal utilization of resources. The CDS could be entrusted with the task of defense planning, subject to overall guidance and directions from the Defense Planning Committee.
- **Lack of co-ordination between the Government and Armed forces:** The **KRC Report** pointed out that in India, the armed forces headquarters is outside the apex governmental structure, therefore, the top executives do not have the benefit of the views and expertise of military commanders, which hurts India’s position in critical war like situations.
- **To further defense diplomacy:** Presently, the crucial aspect of defense diplomacy is being conducted in an ad-hoc manner without an overarching policy direction from the Ministry of Defense. It would be ideal if the CDS is made responsible for all aspects of defense diplomacy, subject to clear policy guidelines from the government.
- **Need for capital procurement:** The armed forces play a vital role in arms procurement. The CDS would be ideally suited to have larger delegated financial powers, over and above those exercised at the lower level, to expedite the procurement process.
- **Needed for quality assurance:** The Department of Defense Production (DDP) is often accused of conflict of interest because of its dual responsibility of being the administrative department for both production and quality assurance, however with the CDS coming up, it would be **ideally suited to take up this responsibility of quality certification**.
- **Resource crunch:** Duplication of assets in infrastructure and human resources, whether in training or in operational commands, is a huge drag on the defense budget, leaving scant little for capital acquisition. **CDS is therefore needed to help cut back infructuous spending in defense.**

Related News

Initiative to improve Combat Readiness: Integrated Battle Groups (IBGs)

- IBGs are brigade-sized, agile, **self-sufficient combat formations, which can swiftly launch strikes against adversary in case of hostilities.**
- The IBGs are to perform both **offensive roles**, involving cross-border operations, **and defensive roles** to withstand an enemy attack.
- Each IBG would be **tailor-made** based on **Threat, Terrain and Task** and resources will be allotted based on the three Ts. They need to be **light so they will be low on logistics.**

Conclusion

In the fast-changing security and defence environment, the country expects a payoff in the form of leaner and meaner forces, who will obtain synergy through planning, training and executing joint operations. Thus appointment of CDS is undoubtedly a bold and decisive step in reforming India’s higher defence management.

7.5. THEATRE COMMAND IN INDIA

Why in news?

Recently, India’s Chief of Defence Staff Gen Bipin Rawat had announced that India may restructure its military organization by creating theatre commands (much like the ones China and the US currently have).

More on news

- The reorganization is expected to be under five theatre commands by 2022 with defined areas of operation and a seamless command structure for synchronized operations.
- The **5 theatre commands** will be made on following lines:
 - A China specific **Northern Command**
 - A Pakistan specific **Western Command**.
 - A **Peninsular Command** covering rest of the land area.
 - A full-fledged **Air Defense Command**.
 - A **Maritime Command** (which will encompass the tri-service Andaman and Nicobar Command).

What is a theatre command?

- Theaterisation or Theatre Command means putting specific number of personnel from **the three services** —army, navy and air force— under a **common commander** in a **specified geographical territory**.
- Creation of theatre commands would **replace the current system of ‘individual service regional commands’**. (India has 19 predominantly single-service commands who operate in their respective geographical areas.)

What are the advantages of creating Theatre Commands in India?

- **Countering China:** Creation of theatre commands could increase the coordination among the forces operating in the region and simultaneously increasing the logistical ability of the forces in the region.
- **Absence of Synergy:** There is absence of synergy among the three forces which lead to poor coordination and duplication of effort. For instance, currently, the Indian Army, Indian Air Force and the Indian Navy all defend Indian airspace on separate communication frequencies.
- **Integration of resources:** The geographical expanse of theatres in India demands unified commands for strategic decisions and critical outcomes that may become possible in concentrated employment of resources.
 - **Integration of logistics by the formation of a Joint Logistics Command** is another potential avenue by which reduction in expenditure can be achieved and the existing resources can be more efficiently utilized.
- **Integrated approach towards procurement,** sans capital acquisitions, the requirements of the military as a whole would be able to be formulated. This in turn would hopefully be the end of the piecemeal approach to purchases done by individual services on an urgent/emergency basis at higher prices, and lead to significant cuts in the cost of maintenance and management of assets.
- **Potential to make the forces leaner:** About 28% of Ministry of Defense’s 2020-21 budget was allocated to pensions, and another 40% of it going toward payment salaries and allowances. Reducing redundancies across the services by integrating manpower within theatre commands has the potential of redirecting a sizeable portion of this allocation towards maintenance and modernization of equipment and capabilities.

Challenges in creation of Theatre Commands

- **Limited experience in theatre command-based organization:** India has had theatre command experience in limited regions like the Andaman and Nicobar Command. This limited experience may require multiple “mid-course corrections” in its implementation.
 - Previous experiences where India has operated in theatre commands, like in Indian Peacekeeping Forces (IPKF) in Sri Lanka, the experience has not been very successful.
- **Unclear structure of command:** It is unclear that who will report to whom within the tri-services and joint theatre command configurations, and who will have operational command over personnel and machinery, service chiefs or theatre commanders.
- **Shortage of resources within the Indian Air Force (IAF):** Airforce has only 31 operational squadrons which would make it difficult for the IAF to permanently station assets in a particular command with territorial boundaries.
- **Possibility of inter-services competition** wherein each service zealously oversees its own assets and strives for a greater share of the defense budget and influence might prove to be an obstacle in creating synergy among the services.

- **Perception of dominance of Army:** Among the three services, the Army has always been the most visible and its officers represented more in leadership positions of joint military institutions, this has created skepticism among other services vis-à-vis reorganization in theatre commands.

Way Forward

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

- Shifting to theatre command would require large scale military equipment, this would require **development of military-industrial complex** to ensure self-sufficiency.
- Change in command structure would require **simultaneous changes in the Military-civilian decision-making structure**. Without these reforms bureaucratic hurdles may render this reorganization counterproductive.
- The government **must evaluate the efficacy of the current Integrated Defence Headquarters including the two joint commands** — the Strategic Forces Command and ANC (Andaman and Nicobar Command). This evaluation can help us premeditate the potential problems in implementation and generation of potential solutions.
- **Increasing Defense Spending:** Both China and USA spend more than 3% of their GDP on Defense and India spends less than 2% of its GDP on Defense. This leads to a scenario of shortage in personnel, equipment and firepower. Without increased spending, moving to a theatre command may create a rigid divide within already stretched military resources

“ The Secret To Getting Ahead Is Getting Started ”



ALTERNATIVE CLASSROOM PROGRAM *for*

GENERAL STUDIES

PRELIMS & MAINS 2022 & 2023

DELHI

Regular Batch	Weekend Batch
25 Nov 10 AM	21 June 9 AM
27 Oct 5 PM	

- Approach is to build fundamental concepts and analytical ability in students to enable them to answer questions of Preliminary as well as Mains examination
- Includes comprehensive coverage of all the topics for all the four papers of GS Mains, GS Prelims and Essay
- Includes All India GS Mains, Prelim, CSAT and Essay Test Series of 2021, 2022, 2023
- Our Comprehensive Current Affairs classes of PT 365 and Mains 365 of year 2021, 2022, 2023 (Online Classes only)
- Includes comprehensive, relevant and updated study material
- Access to recorded classroom videos at personal student platform

Scan the QR CODE to
download **VISION IAS** app



8. EMERGING DIMENSIONS OF WARFARE

8.1. HYBRID WARFARE

Why in News?

Recently, a Chinese data company-Zhenhua has harvested information on millions of people, allegedly on behalf of Beijing's intelligence services, possibly engaging in early stages of 'hybrid warfare'.

More on news

- Zhenhua uses cyber tools to **identify key individuals in its client's opposition**. It uses various tactics, like scraping information off public databases, social media etc. to track digital footprint of individuals.
- It keeps track of institutions and groups related to the individual as well – something that it does by **establishing a 'relational database'** between the individuals that are being surveilled.
- This exercise helps the company **tie down critical aspects in India**, such as **political alliances** between individuals, behavioral traits among key personalities, extent of influence that a person holds.

What is Hybrid Warfare?

Hybrid warfare is an emerging, but ill-defined notion. It generally refers to the use of unconventional methods as part of a **multi-domain warfighting approach**. These methods aim to **disrupt and disable an opponent's actions without engaging in open hostilities**. Following can be cited as its general characteristics:

- The methods adopted by it are a combination of activities, including **disinformation, economic manipulation, use of proxies and insurgencies, diplomatic pressure** and **military actions**. For example, Russia's use of gas and lending instruments in the Ukrainian conflict.
- It tends to **target areas which are highly vulnerable** and where maximum damage can be caused with minimum effort.
- It **usually involves non-state actors** indulging in subversive roles supported by states in order to give the latter some plausible deniability.
- **Other examples** closer to the idea of hybrid warfare are Iran's activity in Syria and ISIL's activities in Syria and Iraq.

Why state and non-state actors are resorting to Hybrid Warfare?

- Hybrid warfare uses a wider set of military, political, economic, civilian and informational instruments which are usually **overlooked in traditional threat assessments**.
- It **targets vulnerabilities across societies** in ways that we do not usually think about.
- It **synchronizes attacks** in novel ways. For example, an urban gathering can experience a simultaneous cyber-attack and a 'lone-wolf' attack, which if synchronized could cause large scale damage to life and property.
- It can be tailored according to the circumstances to **stay below certain detection and response thresholds**, including international legal thresholds, thus hampering the decision-making process and **making it harder to react to such attacks**.
- A hybrid warfare campaign **may not be discovered until it is already well underway**, with damaging effects having already begun degrading a target's capability to defend itself. For example, 2008 Mumbai attacks and a series of 'lone wolf' attacks in Europe were only discovered when they started happening.

Why Hybrid Warfare target the urban spaces?

- Urban spaces due to their **large populations and economic vibrancy** provide **ample opportunity for terrorists and non-state actors** to sneak in and inflict large scale damage to terrorize populations through **"shock and awe" tactics**.
- **Traditional armed forces are ill-trained** and equipped to **fight in crowded urban areas** with large civilian populations.
- Conventional warfare demand direct and complete engagement with the adversary. Hybrid Warfare **uses proxies as indirect tools** creating a **scenario of limited warfare**.

How Hybrid Warfare and Hybrid Threats are potential issues for India?

India has been at the receiving end of variants of Hybrid Warfare. Firstly, from Pakistan in the form of **state-sponsored terrorism** and the other through **cyber-threats from China** akin to the one associated with

Zhenhua. But increasing inclination towards Hybrid Warfare from both state and non-state actors can lead to following issues:

- **New forms of terrorist attacks:** The idea of Hybrid Warfare encourages new forms of terrorist attacks such as **'lone-wolf' attacks** and creation of **'sleeper cells'**. These attacks are extremely difficult to detect and, in most cases, the financial and ideological source remains anonymous.
 - Adversary could also act on the lines of **radicalization of the population**, which leads to issues like **Communalism, Naxalism and Separatism** in the long run.
- **Cyber-attacks:** An adversary can pressure the government to concede to its demands by threatening devastating cyber-attacks aimed at the civilian population. Examples include attacks on networks governing hospitals or electricity and water supplies.
 - India has also been in the line of fire of **Pakistan-backed cyberattacks**. After the abrogation of Article 370, cyberattacks on Indian institutions increased, with many of the attackers openly acknowledging their allegiance to Pakistan.
- **Interference in electoral processes:** Use of techniques from campaigning through the media and social networks to securing financial resources for a political group may indirectly influence the outcome of an election in a direction that favors the adversary's political interests.
- **Disinformation and fake news:** An adversary can create a parallel reality and use falsehoods to **fuel social fragmentation**. The idea behind this is to disorient the public and make it difficult for a government to seek public approval for a given policy or operation.
- **Financial influence:** An adversary can make investments, conclude unfavorable energy-supply deals, or offer loans that make a country vulnerable in the long run to political pressure. For example, the recent steps by Chinese companies to aggressively acquire Indian companies through FDI route in the background of COVID-19 could fall under this category.

What can be done to combat Hybrid Warfare?

Hybrid Warfare is a multi-pronged warfare methodology, thus, to effectively negate it, the response should also be **holistic in nature**:

- **Institutional measures:** to keep vulnerabilities in check and estimate possible hybrid threats.
 - **Conduct a self-assessment** of critical functions and vulnerabilities across all sectors and ensure regular maintenance. For example, regularly **upgrading critical Fintech systems** in the country.
 - **Enhance traditional threat assessment activity** to include non-conventional political, economic, civil, international (PECI) tools and capabilities.
 - **Creation of multinational frameworks** - preferably using existing institutions and processes - in order to facilitate cooperation and collaboration across borders.
- **Training of armed forces:** as in hybrid warfare, armed forces have a dual role of protecting civilian population and disabling enemy. Following techniques can be adopted:
 - Training in **special battle techniques**, as well as conditioning to overcome **urban combat stress**.
 - Training in use of **technological tools** such as smart robots, Unmanned Aerial Vehicles (UAVs)
 - **Intelligence tools** like **Real Time Situational Awareness (RTSA)** for precise operations.
- **Strengthening the democratic institutions:** enables government to **gain trust of its citizens**. This helps government **negate various forms of hybrid warfare** such as disinformation and radicalization.
 - **Inclusion of Civil Society Institutions** such as think tanks multiply the government's capabilities to counter such threats.
 - **Investing in Journalism to raise media literacy:** Global research shows that 70 percent of uses of the term "hybrid threats" by the media are inaccurate. As a result, investing in journalism will indirectly help citizens in understanding the threat.

8.2. SPACE WARFARE

Why in news?

The U.S. and the U.K. recently accused Russia of test-firing an anti-satellite weapon in space raising concerns of space warfare.

About space warfare

- Space warfare is combat that takes place in outer space. The scope of space warfare includes:



- **ground-to-space warfare**, such as attacking satellites from the Earth;
- **space-to-space warfare**, such as satellites attacking satellites; and
- **space-to-ground warfare**, such as satellites attacking Earth-based targets.
- Advent of Space Warfare **began in 1962** when the US exploded a ground-based nuclear weapon in space, which eventually led to the **Outer Space Treaty of 1967**.
- **Existing and Future Space Weapons:**
 - **Kinetic physical weapons:** These weapons attempt to strike directly or detonate a warhead near a satellite or ground station, such as **Anti-satellite weapons (ASAT)**.
 - **Non-kinetic physical weapons:** These are weapons that can have physical effects on satellites and ground stations without making physical contact, e.g. lasers, **high-powered microwave (HPM) weapons**, and **electromagnetic pulse (EMP) weapons**.
 - **Electronic attack:** They target the means through which space systems transmit and receive data by jamming or spoofing radio frequency (RF) signals.
 - ✓ Spoofing is a form of electronic attack where the attacker tricks a receiver into believing a fake signal, produced by the attacker, is the real signal it is trying to receive.
 - **Cyber-attacks:** They can target satellites by monitoring data and traffic patterns, or by inserting false or corrupted data in the system.

Outer Space Treaty (OST), 1967

- It is a **multilateral treaty** that provides the basic framework on **international space law**.
- It is administered by the **United Nations Committee on the Peaceful Uses of Outer Space**.
- **India** is a signatory to this treaty, and ratified it in 1982.
- **Key principles of the OST**
 - **Freedom of exploration and use of space** for the benefit and interest of all countries
 - **Non-appropriation of outer space**, including the Moon and other celestial bodies, by any nation
 - **Prohibition of the deployment of nuclear weapons** or other kinds of weapons of mass destruction in outer space.

Other international treaties for regulation of outer space

- **Moon Agreement, 1979:** It ensures that the Moon and other celestial bodies are used exclusively for peaceful purposes and that their environments are not be disrupted.
- **Liability Convention of 1972** establishes the standards of liability for damage caused by space objects
- **Registration Convention, 1975** requires States to register all objects launched into outer space with the United Nations.
- **Partial Test Ban Treaty (PTBT)** prohibits all testing nuclear weapons in the outer space.
- **Artemis Accords" for Responsible Space Exploration:** Artemis Accord are a series of bilateral agreements between NASA and its international partners that want to cooperate on Civil Space Program.
 - The Accord is **based on the Outer Space Treaty of 1967**.
 - France, Japan, Australia and Canada have already shown their support. **India has not clarified its stand yet.**

Global developments that may impact peace in Space

- **USA's Space Force:** US transformed its Air Force Space Command into the U.S. Space Force, dedicated military branch to help protect the interests of the USA in space, deter aggression etc.
- **France released its first French Space Defense Strategy** in 2019.
- **Iran** recently announced that it has successfully launched a **military reconnaissance satellite**, called **Noor (Light)**.
- **Rendezvous and proximity operations (RPOs)** conducted by **U.S.A., China and Russia** has raised suspicion of respective satellites being used for surveillance or as weapons.

Factors responsible for a potential arms race in space

- **Centrality of space in national security and defense:** Early-warning assets, remote-sensing satellites and weather satellites are critical for national defense.
- **Rapid developments in space technology:** Emergence of micro and nano satellites, higher maneuvering capabilities among satellites, satellite jammers, compact spy satellites, improved cyber infrastructure etc. have significantly enhanced capacity of a nation to partake in offensive and defensive space operations.
- **Protecting commercial interests in outer space:** Mining and commercial exploitation of asteroids and celestial bodies have potential of becoming a domain of geopolitical contestation.
- Space being viewed as **another war fighting domain**.
- **Absence of a strong international treaty** to counter weaponization of space.
- Low levels of transparency and **dual-use nature of space program**.

Possible consequences of a war in outer space:

- **Space debris:** Any missile that smashes into a satellite would disperse thousands of bits of debris. This can trigger **Kessler syndrome** where the debris created from these collisions would create even more debris and continue having a cascading effect.
- Widespread **economic losses** due to destruction of expensive and critical space infrastructure.
- Potential of inflicting extensive **damage to life and property**
- **Difficulties in resolution of conflicts** as certain kinds of attacks in space will not be easily attributable to any one state or non-state actor.
- Risk of a **full-fledged war**.

Way Forward

- **A new space treaty is needed:** with features such as robust verification mechanisms on the deployment of space weapons, the principle of non-interference, proximity rules on how close satellites can maneuver to each other, mechanisms of data sharing, missile test notifications and cooperation in the removal of space debris.
- **Arms control agreements** can also be used to prohibit placement of offensive or defensive weapons in space and restrict testing of ASATs to control space debris.
- **Greater cooperation among nations:** with respect to sharing of technological capabilities of satellites that are located closely or pass each other regularly.

India's Counter space capabilities

- **Mission Shakti:** In 2019, India became the fourth country, after **United States, Russia and China**, to successfully test a direct-ascent anti-satellite (ASAT) missile that targeted a satellite in Low Earth Orbit.
 - It demonstrated its **capability to interdict and intercept a satellite in outer space** based on complete indigenous technology.
- **Defence Space Agency (DSA)** was established to command the space assets of the Army, Navy and Air Force, including the military's anti-satellite capability.
 - It is also to formulate a strategy to protect India's interests in space, including addressing space-based threats.
- **Defence Space Research Organisation (DSRO)** was also created to provide technical and research support to DSA.
- **IndSpaceEx** (simulated space warfare exercise) was conducted in 2019 to identify key challenges and shortfalls if a conflict escalates in space dimension.

8.3. DIRECTED ENERGY WEAPONS (DEWS)

Why in news?

Recently, Defense Research and Development Organisation (DRDO) announced that it plans to develop directed energy weapons (DEWs) under a project named ADITYA.

More on news

- The **Centre for High Energy Systems and Sciences (CHESS)** and **Laser Science & Technology Centre (LASTEC)**, two DRDO laboratories, are working on the DEW projects.
- India has developed a **national plan with short-, medium- and long-term goals** to develop a series of DEW variants with up to 100 kilowatts of power.

What are Directed Energy Weapons?

- The DEWs broadly encompass two fields which are: **high-energy lasers (HELs)**; and **high-power microwaves (HPMs)**—millimeter waves and microwaves. DEWs generally would cover all weapons systems including electronic jammers to lasers.
- How it works:
 - **A DEW emits energy in an aimed direction** without the means of a projectile.
 - It transfers energy to a target and **introduces uneven heat stresses**, leading to failure of structural integration of the target and **causing its destruction**.
 - This weapons effect on humans may be **changed from lethal to non-lethal**.
- Among the two types of DEWs stated above, **HEL has gained** more emphasis at present due to **ease in deployability and low operational cost** as compared to other options.

What are the advantages of DEW over Kinetic Energy Weapons (KEWs) like missiles?

- **Travels at the speed of light** (greater than all the future, present and past conventional weapons) and no complicated calculation for target movement necessary.
- **Not affected by gravity** (no trajectory calculations required).
- **Can be invisible and silent**; attacker remains concealed.
- **Duration for deployment—a few seconds to a minute**—reduces exposure of launcher to enemy position.
- **Recharging of magazine non-existent**, only source of energy required.
- No recoil as there is no momentum, so equipment mountings need not be large. Thus, **can be placed in a smaller area resulting in multiplied stealth capabilities.**
- **Operation range larger than conventional weapons.**

What are the limitations in usage of DEW?

- **The target has to be in the line of sight** of the laser.
- Due to divergence, an inherent property of a beam of light, the **range gets restricted to a few 100 km and not beyond.** Although, technological advances are being worked out to increase range.
- **Presently, the requirement of energy source is large**, but with advancement in superconductivity and nanotechnology, this problem is being worked upon.
- **The beam can be scattered by creating a smoke screen over the target**, placing reflective surfaces, spraying water, etc.

The direct corollary of these limitations is that DEW cannot be an alternative to KEWs. It has to co-exist and complement the Kinetic Energy Weapons (KEWs). But since, the only weapon system capable of disabling, denying, damaging or destroying a nuclear weapon as well as an ICT equipment are DEWs, it becomes eminent for countries to pursue their development.

What are India's motivations behind development of DEW?

- **China factor:** Development of DEWs is seen as particularly important in the context of India's worsening security environment, especially its ties with China. China is also developing DEW technologies. Which makes it imperative for India to develop these technologies as a defence.
- **Potential weapons of the future:** From an operational and strategic perspective, DEWs are weapons of the future. Security experts are of the view that once they are developed to a certain level, the ability to effectively target the incoming unmanned UAVs and drones which currently are doing extremely well in the Armenia-Azerbaijan war will increase manifold.

India's DEW Capabilities

While India is still in the early stages of developing this technology and nowhere near possessing an operational capability, advances in such technologies will have implications for both national and regional security. Following information is available in public domain vis-à-vis DEWs:

- DRDO has developed a **vehicle-mounted high-power laser-directed energy system** for use against drones.
- **A Chemical Oxygen Iodine Laser (COIL)** as a 30-100KW vehicle-mounted gas dynamic high-power laser-based DEW by LASTEC is under development too.
- India is also reported to have developed a system called **KALI, or "kilo ampere linear injector,"** a linear electron accelerator for targeting long-range missiles. KALI has been developed by the DRDO and the Bhabha Atomic Research Centre (BARC).
- In order to make current nascent capability operational in a short period of time, DRDO is in the process of eventually **involving the burgeoning private sector in the R&D works.**

9. MISCELLANEOUS

9.1. PIRACY IN THE INDIAN OCEAN REGION

Why in news?

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

More on news

- The DCOC, **established in 2009 under International Maritime Organization**, is aimed at **repression of piracy and armed robbery against ships** in the Western Indian Ocean Region, the Gulf of Aden and the Red Sea.
 - Jeddah Amendment significantly **broadened the scope of the Djibouti Code** when it was adopted at a high-level meeting in Jeddah, Saudi Arabia in 2017.
 - The members also cooperate in the **investigation, arrest and prosecution** of persons suspected of having committed acts of piracy, the **interdiction and seizure** of suspect ships, the **rescue of ships and people** subject to piracy and armed robbery, and the **conduct of joint operations**.
- It is a grouping on **comprising 18 member states** adjoining the **Red Sea, Gulf of Aden, the East Coast of Africa and Island countries** in the Indian Ocean Region.
- As an observer, India will be looking forward to working together with DCOC/JA member states towards **coordinating and contributing to enhanced maritime security** in the Indian Ocean Region.

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

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

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

- Threat to **national and regional economies** in the form of trade hinderance. For example, Africa’s key maritime routes (Sea Lanes of Communications) are affected adversely as over 90% of Africa’s imports and exports are moved by sea.
- Most of the **piracy intentioned attacks** have been against ships involved in **oil and gas transportation**, such as tankers, bulk carriers and tugs. Apart from that, **commercial ships** from smaller countries and **fishing vessels** have also been targeted by the pirates. For example, The coastline off Nigeria saw the most attacks in 2018. This is partly because of “**petro-piracy**”, **targeting tankers from Nigeria’s rich oil and gas fields**.

The piracy threat in the **Indian Ocean region** was **primarily recognized in 2008 by United Nations Security Council (UNSC) resolution for counter-piracy operations**. At the time, piracy was considered a major threat to both local and global peace and security. Since then, following developments have happened:

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



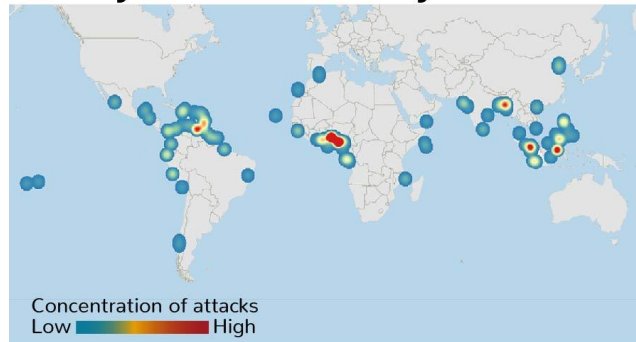
- The purple area referred in the infographic, earlier part of HRA, now comes under the Voluntary Reporting Area (VRA).
- Among the **seafarers affected from piracy** in this region, around **half are from the Philippines, followed by India, Ukraine and Nigeria.**

Global Situation vis-a-vis piracy: One Earth Future Report

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

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

Piracy and armed robbery at sea 2018



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

A large percentage of **India's trade, including oil and fertilisers**, passes through the Gulf of Aden. The estimates suggest that, **Indian imports** through the Gulf of Aden route valued in the **order of USD 50 Billion and exports at USD 60 Billion.** The safety and unhindered continuity of maritime trade, through ships that use this route, is a primary national concern as it directly impacts our economy. In the light of this, following steps have been taken by the Government:

- **Legislative efforts** in the form of Anti-maritime Policy Bill 2019. Following can be cited as the key features of the Bill-
 - The Bill defines piracy as “**any illegal act of violence, detention, or destruction committed against a ship, aircraft, person or property, for private purposes, by the crew or passengers of a private ship or aircraft**”.
 - **Applicability of the Bill:** All parts of the sea adjacent to and beyond the limits of the Exclusive Economic Zone of India.
 - **Extraditable Offence: Piracy accused can be transferred to any country for prosecution** with which India has signed an extradition treaty. In the absence of such treaties, offences will be extraditable on the basis of reciprocity between the countries.
 - **Designated Courts:** Central Government, in consultation with the Chief Justice of the concerned High Court, will specify certain courts as Designated Courts for speedy trial of offences of piracy.
- **Escort and protection:** The Indian Navy commenced anti-piracy patrols in the Gulf of Aden from 2008.
 - **Indian Naval and Coast Guard ships have also been deployed** in piracy prone areas nearer the Indian coast. **Around 1000 plus ships of various nationalities have been escorted** and more than 40 piracy attacks prevented by Indian forces till date.
 - The Director General Shipping has launched a **web-based registration service** where merchant ships can register with DG Shipping in order **to avail of the escort facility** provided by Indian Naval ships in the Gulf of Aden.
- **Global coordination:** By participating in the multilateral for a setup to combat piracy.
 - India is an active participant of various mechanisms like “**Shared Awareness and De-confliction (SHADE)**” that have been established to **facilitate sharing of information.**
 - **India, Japan and China** (all three nations operate independently) have agreed to **coordinate patrols** thereby ensuring an effective and **optimum use of the combined maritime assets to escort ships**, especially in the Internationally Recommended Transit Corridor established for use by all merchant ships in the Gulf of Aden.

Need for such a legislation

- **To bring a comprehensive, and a specific domestic legislation** on piracy: Till now, the provisions of the Indian Penal Code and the Admiralty jurisdiction of certain courts have been invoked.
- **To deal with increasing incidences of piracy**, within India's Exclusive Economic Zone.
- **To fulfil India's commitment** in signing the United Nations Convention on the Law of the Sea (UNCLOS).
- **To promote the safety and security of India's maritime trade** including the safety of our vessels and crew members.

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

- **Contact Group on Piracy off the Coast of Somalia:** It was established in 2009 as a voluntary, ad hoc international forum to coordinate international efforts in the fight against piracy off the coast of Somalia.
 - As of now, **over 60 nations and international organizations participate in the CGPCS.**
- **Maritime Security Programme (MASE):** It is a European Union-funded programme to promote Maritime Security in Eastern and Southern Africa and Indian Ocean. Under MASE, the Indian Ocean Commission (IOC) has established a mechanism for surveillance and control of the Western Indian Ocean with two regional centres in Madagascar and Seychelles.
- **Maritime Crime Programme (MCP) - Indian Ocean:** The Indian Ocean team within the **United Nations Office on Drugs and Crime's (UNODC) Maritime Crime Programme** assists states in the Indian Ocean region to enhance and coordinate their efforts to combat maritime crime, with a **focus on criminal justice capacity building.** Following can be cited as its key facets:
 - **Regional "Piracy Prosecution Model":** It provides a 'legal finish' to counter-piracy operations.
 - **Piracy Prisoner Transfer Programme:** It aims to facilitate the transfer of consenting persons convicted of piracy in regional States to UNODC supported prisons in Somalia.
 - **Activities beyond counter-piracy support:** MCP Indian Ocean programme continues to work with regional States to enhance their capacity to combat a wide range of maritime crimes like drug trafficking.
- **Other important regional efforts** include **African Union's Lomé Charter** and **Yaoundé Code of Conduct** which is active in West and Central Africa.

Addressing the root cause: The way forward

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

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

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

Learning from Puntland State of Somalia

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

9.2. MILITARIZATION OF ANDAMAN AND NICOBAR ISLANDS

Why in news?

The Ladakh stand-off with China has catalysed India's efforts to strengthen its military presence at the Andaman and Nicobar Islands (ANI).

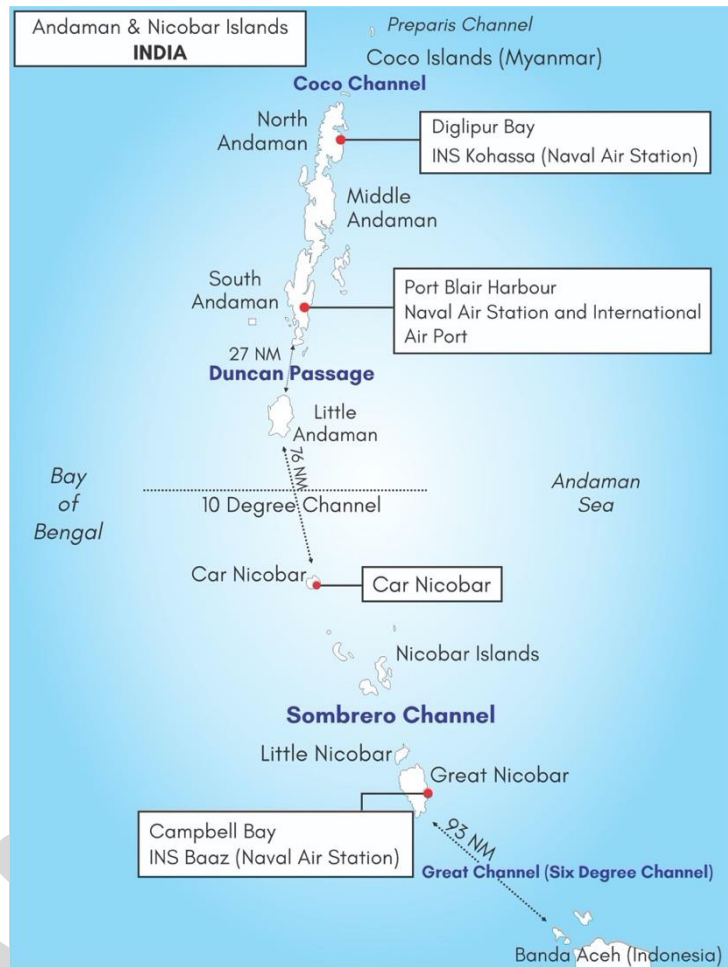
More on news

- Government **plans for basing additional military forces**, including facilities for additional warships, aircraft, missile batteries and infantry soldiers at the strategically located Andaman Islands.
- **Runways at Naval air stations INS Kohassa in Shibpur and INS Baaz in Campbell Bay are being extended** to support operations by large aircraft.
- Indian strategic commentators are even recommending to **permit friendly foreign navies access to the ANI's military bases.**

Need to militarize ANI

- **Growing Chinese presence:** In recent years, China strengthened its overall presence in **Indian Ocean Region (IOR).**

- Examples include deployment of a submarine at Colombo harbour, developing naval bases at Gwadar and Djibouti etc.
- **Strategic location:** These islands help India to defend its vital stakes in IOR. To achieve the purpose, India has set up Andaman and Nicobar Tri service Command.
- **Economically important:** These islands dominate the Bay of Bengal which contains important sea lines of communication. **More than 30 percent of the world's seaborne trade passes through this narrow region.**
 - They comprise 30 per cent of India's Exclusive Economic Zone (EEZ).
- **Buffer Zone:** These Islands act as a buffer zone between India and rest of the nations present in IOR.



Challenges in Militarizing ANI

- **Lack of clarity in approach:** On the matter of the strategic development of the Andamans, **India's defence and foreign policy establishments have not always been on the same page.** This act as a barrier in development of security infrastructure on the islands
 - Given the complexity of India-China bilateral relations, these strategic interactions at the A&N Islands may rile China and lead to further antagonism between the two countries.
 - Many countries in neighbourhood consider India as a benign and benevolent power. Power projection at islands will change this perception of India.
- **Lack of Infrastructure & Communication:** After several years, an undersea cable link between India's mainland and the islands remains incomplete.
 - Recently, **Submarine Optical Fibre Cable (OFC)** connecting Chennai and Port Blair was laid down to provide connectivity to Andaman & Nicobar Islands. It will enable delivery of faster and more reliable mobile and landline telecom services to Andaman & Nicobar Islands.
- **Islands are inhabited:** Of the 572 islands that make up the Andaman and Nicobar group, only 37 are inhabited. The absence of a human presence on hundreds of these islands has made them vulnerable to narcotics smuggling, intrusion by foreign vessels, and other incursions.
- **Geographic factors:** Heavy rainfall restricts building activity to six months a year and the distance from mainland adds to the cost of construction as all material must be shipped to the islands.
- **Sensitive ecology:** Environmentalists warn that the recent infrastructure projects (as planned by NITI Aayog such as hotels, resorts and a trans-shipment hub at Campbell Bay) could devastate the fragile ecology of the Andaman. Already many islands are facing significant damage from the climate crisis.

Way forward

- India should follow the principle of **'strategic autonomy'** while taking its decision to militarize ANI

India's presence in Indian ocean:

- **Military Exercises:** MILAN, MALABAR
- **Logistics-sharing agreements:** with the US and Australia, as well as with France, Singapore, and South Korea. A similar logistics-sharing agreement with Japan is in an advance stage of negotiations. Examples include: Logistics exchange at ports Sabang, Changi, Duqm, Agalega, Chabahar etc.
- **A&N Command:** It is the first and only Tri-Service theatre command of the Indian Armed Forces. It patrols India's EEZ to suppress gun running, narcotics smuggling, piracy, and poaching, and conducts maritime surveillance and Humanitarian Assistance and Disaster Relief (HADR) operations.

- Strategic autonomy denotes the ability of a state to pursue its national interests and adopt its preferred foreign policy without being constrained in any manner by other states.
- There is a **need to encourage migration from the mainland** and open up some of these strategically located uninhabited islands to tourism. That would give India a stronger physical footprint and would help the country track the movement of vessels and people.
- While developing islands, India **needs to ensure that ecology of the place remains preserved**.

9.3. INDIA'S NUCLEAR DOCTRINE

Why in news?

Recently, India at the UN Conference on Disarmament 2020 reiterated its commitment to the nuclear doctrine of “No First Use” against nuclear weapon states and non-use against non-nuclear weapon states.

What is meant by nuclear doctrine and what are the major aspects of India's nuclear doctrine?

A nuclear doctrine of any nuclear weapon country **encompasses the goals and missions that guide the deployment and use of nuclear weapons** by that country both during peace and war. The **dominant goals of a nuclear doctrine** most often include deterrence, target destruction, assurance of allies, and a hedge against an uncertain future.

- India's nuclear doctrine is **centred around deterrence rather than war-fighting** capability. Major aspects of Indian Nuclear Doctrine can be summarized as follows:
 - **Building and maintaining a credible minimum deterrent:** Assuring adversary nation's belief that the costs of launching a nuclear strike against India would be unbearable and unacceptable.
 - **A posture of No First Use (NFU):** Nuclear weapons will only be used in retaliation against a nuclear attack on Indian territory or on Indian forces anywhere.
 - **Massive Retaliation:** Indian response to a nuclear strike is massive retaliation to inflict incalculable and unacceptable damage to the aggressor.
 - **Political Control of Nuclear Weapons:** Nuclear retaliatory attacks can only be authorised by the civilian political leadership through the Nuclear Command Authority (NCA). The **NCA comprises a Political Council and an Executive Council**.
 - **Conditional use of nuclear weapons:** Non-use of nuclear weapons against **Non-nuclear Weapon States (NNWS)** (Negative Security Assurance) and option of retaliation with nuclear weapons in the event of a major chemical or a biological weapons (CBW) strike against India.
 - **Non-proliferation:** Continuance of strict controls on export of nuclear and missile related materials and technologies and participation in the Fissile Material Cutoff Treaty (FMCT) negotiations.
 - **Commitment to Disarmament:** Moratorium on nuclear tests and continued commitment to a nuclear free world through verifiable and non-discriminatory nuclear disarmament.

India's nuclear capabilities

- India's current **ballistic missiles** including the **Prithvi, the Agni-1 and Agni-2, as well as the Agni-3** have the potential to deliver a nuclear warhead.
 - India has a number of combat aircraft which can be used as delivery vehicle, including the **Jaguar, the Mirage-2000 and the Su-30**.
 - The **nuclear submarine INS Arihant** gives India the maritime strike capability.
- These three launch mechanisms complete what is called the **Nuclear Triad**.

What is India's present nuclear standing vis-à-vis the global nuclear discourse?

India's participation is based on the **progressive nuclear disarmament and adoption of a non-discriminatory & verifiable process to effect this disarmament**. Based on these principles, India's stand on various international treaties and regimes is as follows:

- **India has not signed the CTBT** but maintains a unilateral moratorium on nuclear testing and supports negotiations for a Fissile Material Cut-off Treaty (FMCT) that is "universal, non-discriminatory, and internationally verifiable."
- **India has remained firmly outside of the NPT**, arguing that “nuclear weapons are an integral part of India's national security and will remain so pending the global elimination of all nuclear weapons.
- **India has also opposed** the recent enforcement of **Treaty on Prohibition of Nuclear Weapons (TPNW)** which India believes is **not a comprehensive instrument on disarmament** as it excludes the verification of nuclear armaments.
 - India maintains that the Geneva-based **Conference on Disarmament (CD)** is the **single multilateral disarmament negotiation forum**.

- India has a **facility-specific safeguards agreement in place with the International Atomic Energy Agency (IAEA)** and a **waiver from the Nuclear Suppliers Group (NSG)** allowing it to participate in nuclear cooperation agreements with other countries.
- India has been **actively pursuing membership into the NSG** and has received explicit support for its membership from many current NSG members including the United States, Russia, Switzerland and Japan except China.
- India was **recently accepted as a member of three of the four Multilateral Export Control Regimes;** Missile Technology Control Regime (MTCR) in 2016, Wassenaar Arrangement in 2017 and Australia Group in 2018.
- The Indian mission to the United Nations has also submitted several **draft recommendations on “reducing nuclear danger,”** which include “steps to reduce the risks of unintentional and accidental use of nuclear weapons, including through de-alerting and de-targeting nuclear weapons.”

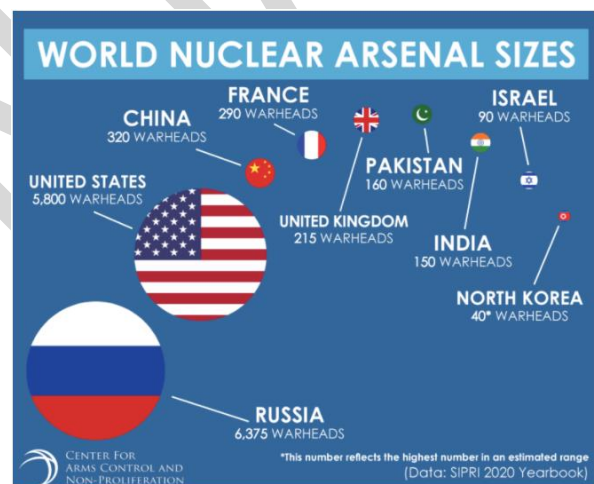
Is India’s nuclear doctrine still relevant in its present form or does it need a review?

India’s existing Nuclear Doctrine has served its aim of creating sufficient nuclear deterrence for its adversaries. But, at the same time, an examination of the existing doctrine has indicated that with the fast changing security dynamics in the region, there is a requirement for updating the existing doctrine. This debate has also gained momentum with recent remarks by the government.

The government in its 2014 election manifesto promised to study, revise and update India’s nuclear doctrine to make it relevant in tune with changing geostrategic realities. In August 2019, Indian Defence Minister implied that India’s no first use policy would not be continued indefinitely.

Following are the reasons that advocate for the review of the doctrine:

- **Periodic review in a constantly evolving and shifting, geo-strategic world order:** The American and the Russian governments review their nuclear policy periodically. The Indian doctrine, however, does not have such a caveat which requires such mandatory scrutiny.
- **Technological advancements in military:** Though India has tried to keep pace with the global technological advancements whether it is Ballistic Missile Defence (BMD) capabilities or the MIRV trajectory; but other technologies can challenge any country’s policy of credible deterrence.
- **Efficacy of No First Use:** NFU remains the **most debated element of India’s nuclear doctrine.**
 - **Those who are against this caveat** believe that NFU may result in unacceptably high initial casualties and damage to Indian population, cities, and infrastructure.
 - **On the other hand, the theorists, who are in favour of NFU view,** believe that India’s strategic restraint posture exemplified by NFU has resulted in major gains internationally, including the lifting of economic sanctions and the removal of technology denial regimes.
- **Emerging nature of threats:** The present doctrine is silent over dealing with threats in the form of ‘Cyber Crimes in the nuclear field’ and ‘Nuclear Terrorism’. Such threats can not only harm the individual interests of nations but also cause a global security risk as a whole.
- **Countering Chemical and Biological attacks:** Critics argue that the option of retaliating with nuclear weapons in case of CBW attack is an **aggressive posture that dilutes the NFU pledge** for NNWS that weakens credibility and ultimately nullifies deterrence. It is also believed that the **source of biological weapons is difficult to ascertain** and also the threat from the NNWS can be countered by conventional weapons.



On what lines can the present doctrine be reviewed?

- **Dedicated defense technology programs:** With India continuously playing defence technological catch-up with other nuclear powers like China, the Nuclear Doctrine does not get the technological support needed for its effective enforcement.

- **Increasing flexibility on ‘massive retaliation’ commitment:** The rationale behind the commitment is to create credible deterrence. But the commitment of massive retaliation forces the political actors to escalate the nuclear war, thus limiting the retaliatory options. To overcome this, some ambiguities could be introduced in the doctrine which enable the country to respond to threats like TNWs without it escalating to a full-fledged war.
- **Synchronizing with Foreign Policy:** The foreign policy continuously changes with the geo-political developments and changing national security needs. Some experts suggest reviewing the nuclear doctrine on the basis of changing foreign policy. This can serve the twin objectives of protecting the nuclear doctrine from becoming obsolete and regular review may serve as an indicator of our current military capabilities and what we need.
- **Building upon its status of a responsible nuclear power** – Given the current uncertain environment, India can emerge as a **potential leader for promoting global nuclear non-proliferation and disarmament.** Following efforts can be made by India in this regard -
 - **Reconsideration of India’s doctrinal positions:** This include adopting a “global NFU” norm instead of a “conditional NFU” (which is India’s current principle).
 - **Engaging in multilateral discussions** at the UN and other parallel platforms to voice the security and non-proliferation issues concerning states like itself. It can also work towards **reviving forums such as Conference on Disarmament.**

9.4. EPIDEMICS AND NATIONAL SECURITY

Why in news?

An epidemic in the form of Covid-19 has caused large scale loss of life and disturbed livelihoods all across the world. The magnitude of damage that it has caused has sparked a debate regarding whether epidemics should be treated as a national security problem.

What is National Security?

National Security, in a more traditional sense, refers to the **preservation of the state, its territorial integrity, political institutions, and national sovereignty** from physical threats. But in the modern times the definitions have broadened to include following facets:

- **Law and order problems:** Problems which do not threaten the national security in traditional terms but create a violent situation which in turn creates breeding ground for a National security situation. These are activities like civil war, ethnic conflict, crime and drugs.
- **Economic threats:** They indirectly threaten the developmental dynamics by disturbing the economic processes.
- **Technology driven threats:** Threats like cyber-terrorism, space warfare etc. have assumed increased importance in recent times.
- **Health Security:** Diseases like Tuberculosis, Malaria and HIV are seen as threats to human security because of the enormous loss of life they cause.

India’s National Security Objectives

- Protecting India’s national sovereignty.
- Securing the territorial integrity of India.
- Promoting India’s rise to its rightful place in international affairs.
- Ensuring a peaceful internal environment within India.
- Creating a climate for our citizens that is just, equitable, prosperous, and shields them from risks to life and livelihood.

How do epidemics threaten National Security?

- **Can trigger a violent conflict:** Epidemics may contribute to societal destabilization and in extreme cases it may accelerate the processes that lead to state failure which threatens national security. Various examples of AIDS triggered violence can be seen in Sub-Saharan Africa.
- **Biological weapons:** Biological agents including epidemic diseases can be weapons of war and thereby directly and immediately threaten security. Combatants may deliberately target public health and spread disease to weaken and demoralize an enemy population.
- **Affect bilateral relations:** Outbreaks may prompt disputes among states over appropriate policy responses in a number of areas, including freedom of movement for people and goods. For example, disputes arising during the MERS outbreak between India and countries in the Middle-east regarding Indian diaspora.

- **Human security:** The idea that human security is part of national security directly makes epidemics a threat to nation by threatening its people. For instance, by this approach tuberculosis is a national security threat to India because it threatens health of citizens of this country.

Historical connect: Epidemic and National Security

Historically, epidemic infections have affected national security in various ways on various instances such as:

- Various scholars argue that **Germany's loss in WWI** was at least partly due to the negative effects of the 1918 influenza epidemic.
- In **WWII**, similarly, **malaria** caused more U.S. casualties in certain areas than did military action.
- More recently, **AIDS outbreak** marked the first time that the **UN Security Council** acknowledged the threat that epidemics pose and consequently recommended to expand the definition of national security.

Advantages of viewing epidemics as National Security threat

- **Higher priority:** Associating health policy commitments with security can elevate the level of priority given to an issue and deliver results. Also, it would **make available more resources** to health emergencies via national security channel.
- **Better institutional organization:** A national security problem is more likely to have a well-defined and streamlined institutional apparatus which in turn could generate a more coordinated and accelerated response.
- **Increased global commitment:** Viewing epidemics as a security issue may encourage a deepening of commitment by countries to international cooperation and preparedness.

Challenges in looking at an epidemic through security lens

- **Risk of mislabeling everything as security threat:** If everything that causes a decline in human well-being is labelled a security threat, the term loses any analytical usefulness.
- **This approach relieves developed states:** Viewing epidemics as part of national security relieves states without major public health threats of any moral obligation to respond to health crises of monumental proportions in the developing world. Currently, this is more seen in the perspective of humanitarian aid.
- **Deter regional cooperation:** Issues of National security see relatively lower level of cooperation among neighboring countries. This could directly impede much needed cooperation.

Is India treating Covid-19 as a National Security threat?

The national security matters in India are dealt by National Security Act of 1980. But Covid-19 is being legally dealt by two laws namely the **Epidemic Diseases Act, 1897**, and the **Disaster Management Act, 2005**. In that sense, Covid-19 is not being treated as National Security threat in legal terms as of now.

Way forward

In a nutshell, global pandemics threaten state security in three ways – domestically, economically and militarily. Going forward, while there are valid arguments both for and against treating epidemics as a national security issue, following may also be seen as an alternative -

- **Viewing it as foreign policy issue rather than national security concern:** It may be more fruitful to view disease and health issues as concerns for foreign policy deserving of multilateral responses, rather than as security threats requiring bilateral policy responses.
- **Independent institutional mechanism:** Security labels provide health emergencies with resources; the same human and financial resources could be garnered if an independent institutional mechanism for health emergencies can be created.

Copyright © by Vision IAS

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