APPROACH – ANSWER: G. S. MAINS MOCK TEST - 1411 (2020)

1. Why are shell companies seen as attractive vehicles for those seeking to launder money or conduct illicit activity? Highlight some steps that have been taken by the government in recent times to curb shell companies in India. (150 words) 10

Approach:

- Give a brief introduction of shell companies.
- Discuss the reasons for use of shell companies in money laundering and illicit activities.
- Mention some steps taken by the government to curb use of shell companies.
- Suggest some way forward to further enhance the control on shell companies.

Answer:

A shell company is a corporate entity without real business operations or significant assets and physical presence. Shell companies can be used to hide the ownership, evade taxes and convert black money into white and vice versa. There are various reasons for using shell companies in money laundering and illicit activities involving financial crimes, such as:

- **Hiding source of money**: Shell companies show bogus financial transactions to hide illicitly acquired money and thus transforming black money into white.
- **Anonymity**: Criminals use this anonymity to mask their identities, involvement in transactions, and origins of their wealth, hindering law enforcement efforts to identify individuals behind illicit activities.
- **Evading taxes**: The government does not get any tax because there is no accounting of the black money.
- **Facilitates illicit payments such as bribes**: Many infrastructure companies use shell companies to get cash for paying bribes to various public officers.

Recently, the government busted a major racket of fake invoicing of ₹7,896 crore, involving fraudulent input tax credit (ITC) of ₹1,709 crore, using a network of 23 shell companies. To curb the menace of shell companies, the Government **has taken various steps**:

- **Formation of task force:** In 2017, a task force on shell companies was set up to have a multi-agency approach, which included members from CBDT, ED, CBI etc. to check the menace of shell companies.
- **Identifying and deregistering shell companies:** More than 3 lakhs shell companies have been de-registered.
- **Action against directors of shell companies:** More than 3 lakh directors of defaulting companies were disqualified under the Companies Act, 2013 for non-filing of financial statements and names of about 55,000 were revealed. It is notified that Directors of defaulting companies cannot be reappointed for up to 5 years.
- **Trading restrictions:** Securities and Exchange Board of India (SEBI) has imposed trading restrictions on 331 listed entities, which were identified as shell companies.
- **Use of technology:** Money trail of shell companies is being traced via data mining.
- **Database of shell companies:** Serious Fraud Investigation Office (SFIO) is creating a database of shell companies, and sharing it with all required regulators.

In this context, absence of a proper and uniform definition for shell companies under the legal framework inhibits any concrete action on them. Thus, the government must define a shell company either under the Income Tax Act, 1961 or under the Companies Act, 2013. It will help identify if a company has been set up to launder money or exploit regulatory arbitrage.

2. What is SMART policing? Highlight the reforms required in the current system to realize this vision. (150 words) 10

Approach:

- Briefly describe the concept of SMART policing and its benefits.
- Discuss the reforms that are required to realize this vision.
- Conclude on the basis of above points.

Answer:

Smart policing can be defined by the use of modern technology and processes, which promotes pro-active policing by preventing criminal activity through enhanced police visibility and public engagement. It is the police force, which is, Strict and Sensitive, Modern and Mobile, Alert and Accountable, Reliable and Responsible, Techno-savvy and Trained.

Recently, many steps have been taken in this regard like Police Forces Scheme, specialized wings for social and cyber crimes in several states, various technological reforms including modernization of the control room, fast tracking crime and criminal tracking network and system etc.

However, various reforms/ steps are still required to realize this vision:

- **Legislative reforms:** It includes enactment of a central act against organized crimes, a single Police Act for the country, moving 'police' and 'public order' to Concurrent List, statutory backing for CBI and changes in criminal procedures and evidence systems.
- **Boosting infrastructure and capacity of the police forces:** This can be done by increasing the number of police personnel in the country, improvements in recruitment, training and service conditions including up gradation on one hand and improving the infrastructure, working hours, housing facilities on the other.
- **Administrative reforms:**
  - As directed by the **Supreme Court in Prakash Singh v. Union of India case,** "the investigating police shall be separated from the law and order police to ensure speedier investigation, better expertise and improved rapport with the people.
  - To counter terrorism related emergencies, a **National Counter Terrorism Centre** must be established.
- **Technological scaling**: Fast completion and operationalization of Criminal Tracking Network and System (CCTNS) and National Intelligence Grid (NATGRID) is required. There is a need to have a unique and integrated emergency number as is present in other parts of the world. Space technology can also be used to tackle internal threat e.g. The 'Crime Mapping Analytics and Predictive System' adopted by Delhi.
- **Building partnership with society**: Policing should be made more citizen centric by involving citizens in various policing areas; effectively utilising community policing and establishing partnerships in various forms such as rotary clubs, roping in businesses to increase vigilance in market areas etc.

India is a fast growing economy with growing complexity in society raising several modern threats such as terrorism, radicalization, lynching, left wing extremism, cyber-crimes, data theft, etc. In light of the given circumstances, the government must make police reforms as one of its greatest priorities.

3. Giving a brief account of the Bodoland dispute, discuss the key aspects of the third Bodo Peace Accord. (150 words) 10

Approach:

- In the introduction, briefly mention the reasons that led to Bodo insurgency in Assam.
- List down the provisions of the third Bodo Peace Accord.
- Analyse its role in bringing peace in the conflict regions of Assam.
- Conclude on the basis of above points.

Answer:

Bodoland or the **Bodoland Territorial Area District** (BTAD) is an autonomous region in the State of Assam, comprising four districts (Kokrajhar, Baksa, Chirang, Udalgiri). Bodos are the single largest community among the notified Scheduled Tribes (STs) in Assam and constitute about 5-6% of Assam's population.

Bodo issue in Assam – Demand for statehood and insurgency:

Till the 20th century, Brahmaputra Valley witnessed large-scale in-migration from the then East Bengal and Central Indian Chotanagpur region. To reclaim ethnic and linguistic identities of Bodos, demand for a Bodo state arose in the 1960s and later in the 1980s by the All Bodo Students' Union (ABSU). The armed group Bodo Security Force subsequently renamed itself National Democratic Front of Bodoland (NDFB), and later split into factions.

The ABSU-led movement culminated in a 1993 Bodo Accord, which paved the way for a **Bodoland Autonomous Council** (BAC). In 2003, the second Bodo Accord was signed with the extremist group Bodo Liberation Tiger Force (BLTF). This led to the formation of **Bodoland Territorial Council** (BTC). This third Bodo Peace Accord is a tripartite agreement between the Centre, the Assam government and the four factions of Assam-based insurgent group National Democratic Front of Bodoland (NDFB) signed recently, for bringing lasting peace in the Bodo-dominated areas in Assam.

Key provisions:

- A commission would be formed to determine the boundaries of the Bodo Territorial Area Districts (BTAD). Villages dominated by Bodos presently outside BTAD would be included and those with non-Bodo populations would be excluded.
- Bodos living in hills would be conferred Scheduled Hill Tribe status.
- BTAD would now be called **Bodoland Territorial Region** (BTR) and it would have more executive, administrative, legislative and financial powers.
- Bodo with Devanagari script would be the associate official language for entire Assam.
- Over 1500 armed cadres will abjure violence and join the mainstream.
- Setting up of Bodo-Kachari Welfare Council for development of Bodo villages located outside Bodo Council area.
- Special Development Package of Rs. 1500 crores over a period of three years for all round development of Bodo Culture, Region and Education.

The third Peace Accord includes the more militant NDFB factions, has a more equitable power-sharing arrangement, and seeks a comprehensive and final solution to the Bodo aspirations and demands while keeping intact the territorial integrity of Assam. It needs to be ensured that the political arrangements sustain the elections in the expanded BTC and maintain inter-tribal harmony.

4. What is 'dark net'? How does it pose a security challenge for India? (150 words) 10

Approach:

- Briefly explain what you understand by dark net.
- Briefly mention the areas where it is used.
- Identify the challenges posed by the dark net to India's security.
- Conclude appropriately.

Answer:

The content on Internet can be divided into surface web and and deep web. While surface web can be accessed using search engines, deep web cannot be indexed by search engines.

The dark net or dark web is part of deep web and refers to encrypted networks on the Internet that are not indexed by search engines such as Google, Yahoo or Bing. It is deliberately hidden and accessible only by using special software like Tor (The Onion Router), or I2P (Invisible Internet Project).

The dark net is often used for various purposes such as free access to various resources (academic research papers), maintaining secrecy in communication and guard against leaking and transferring information. However, despite its advantages, the dark net also poses challenges to India's internal security**.**

These include:

- **Illegal activities**: Activities such as sale of drugs and firearms, fake currencies, child pornography, human trafficking etc. are carried out over the dark net. The Narcotics Control Bureau (NCB) recently arrested the country's first 'darknet' narcotics operative, who allegedly shipped hundreds of psychotropic drug parcels abroad in the garb of sex stimulation medicines.
- **Cyber fraud**: Details of bank account holders, registered phone numbers etc. have been reported to be on sale over the darknet, which can lead to identity theft. Group-IB, a cyber security company, revealed that a database containing more than 4,50,000 payment card details of Indian banks has been uploaded on the darknet.
- **Culpability of offence**: It is not illegal to access the dark web. However, its encryption enables the identities and IP addresses of the people accessing the dark web to be untraceable by internet service providers or government agencies. This leads to multiple complexities and loopholes in investigation and establishing evidence.
- **Use of crypto currencies**: Deals done on the darknet are mostly through crypto currencies like Bitcoin. As identities remain anonymous, enforcement agencies are unable to trace those who use the darknet to engage in illegal activities.
- **Terrorism**: Since the surface web is carefully monitored by law enforcement agencies, terrorist organizations like the Al Qaeda have turned to the dark net to spread propaganda, recruit supporters and protect the identities of supporters, raise funds etc. It will be difficult for Indian authorities to trace the activities of the terrorist organizations and their supporters.

In light of these challenges, the Centre for Development of Advanced Computing (CDAC) is working with CSIR on developing a dark net/network telescope-based cyber security monitoring and interference framework. Similarly, Kerala police has established a specialised dark net lab in Cyberdome and some officers have been trained as dark net analysts to monitor these activities. Further, the Indian agencies must collaborate with other countries, monitor greater traffic over the dark net and invest in research and training of personnel in the field of cyber security to deal with it.

5. Given the duties and functions of the Chief of Defence Staff (CDS), discuss why its establishment is being seen as an important defence reform. (150 words) 10

Approach:

- Give a brief background of the post of the Chief of Defence Staff (CDS).
- State the duties and functions of the CDS and highlight the significance of its establishment as an important defence reform.
- Conclude on the basis of the above points.

Answer:

The Chief of Defence Staff (CDS) is a high military office created by the Ministry of Defence that oversees and coordinates the working of the three Services, and offers seamless tri-service views and single-point advice to the Executive on long-term defence planning and management. Various Committees formed for defence and military sector reforms (Naresh Chandra Committee, Shekatkar Committee) had recommended the creation of the post of CDS in India.

The duties and functions of the CDS:

- It will function as the **Permanent Chairman of the Chief of Staff Committee** instead of a rotational chairman.
- It will **head the Department of Military Affairs** and function as its Secretary.
- It will act as the **Principal Military Adviser (PMA) to** the **Defence Minister** on all tri-service matters.
- It will act as the **Military Advisor to the Nuclear Command Authority (NCA)**.

- It will act as **a member of Defence Acquisition Council (DAC)**.

Its establishment is being seen as an important defence reform due to the following reasons:

- This will **ensure jointness in operations, procurement, training** etc. for the services through joint planning and integration of their requirements and establishment of joint/theatre commands.
- Designation of the CDS as the PMA will enable unhindered access to the Defence Ministry, enable **active participation of the military in policy-making** and accelerate the process of decision-making. It will act as the single-point advisor to the Government of India.
- The designation of CDS as an advisor to the NCA will give it a **strong hold in taking nuclear operations decisions** and enhance the credibility of India's nuclear deterrence.
- Making the CDS a member of DAC will promote effective planning, as he/she can assign inter-services prioritisation to **capital acquisition proposals** based on the anticipated budget and **ensure optimal utilization of resources**.
- The CDS will implement the five-year Defence Capital Acquisition Plan and the two-year roll on Annual Acquisition Plans as a follow up of the Integrated Capability Development Plan.

The appointment of the CDS is one of the measures taken by the government to modernize and integrate the armed forces. However, its success depends on the ability of the CDS to synergize the operations of the three armed forces. It should also be complemented by the overhaul of the defence acquisition process, creation of theatre commands, technological upgradation of the forces etc.

6. Data Protection is not just a privacy issue, it is also a national security issue. Discuss.
(150 words) 10

Approach:

- Briefly explaining the concept of data protection, discuss how major focus is given on data privacy in the data protection debate.
- Discuss how it has national security implications as well, using suitable examples.
- Conclude on the basis of the above points.

Answer:

Data protection is the process of **safeguarding important information** from corruption, compromise or loss. However, the debate on data protection is framed mainly as a debate on privacy of the data. For instance, the **Information Technology (IT) Act 2000** and the **draft Personal Data Protection Bill 2019** mainly focus on keeping personal data of citizens secure and protected.

In this context, there have been arguments that the debate about how technology companies collect, handle, share and sell user data and provide access to users should be broader than privacy considerations – that it should take into account national security implications too. That this is an important aspect, which needs focus, is evident from the following:

- It has been argued that the defence and national security apparatus will become increasingly dependent on data-driven services, in the times to come, and for everything from tanks to drones, data will be at the heart of national security.
- Any attempt to sabotage confidential information of government offices, national defence, intelligence agencies etc. has direct implications on national security. For example, leakage of sensitive information on Rafale fighter jets.
- Data held by social media companies and access to their platforms by hostile third parties may provide them with tools to influence public opinion and undermine democratic practices. This has potential security concerns as raised by the Oxford-Analytica report on US elections.
- With many data breach incidents in recent times such as stealing of 1.2 billion pounds from British bank customers by scammers over the last year, the implications for economic security of a nation are huge.
- Data is the fuel behind attacks on critical infrastructure, which may turn into a disaster. The recent cyberattack on Kundankulam Power Plant is one such example.

- Lack of data protection and anonymity is leading to increase in crimes such as phishing scams, extortion, hate speech etc.
- Now, hackers can attack connected cars and insulin pumps etc., thus having critical and direct life-changing, even life-threatening consequences.

No doubt data privacy is an important part of data protection, but it also involves other components such as protecting data from unauthorized users, encrypting data storage, regulating access by third party etc. Considering all these issues, the government is also looking towards other data protection measures, such as the push towards data localization.

7. Highlighting the role of the National Security Guard in India, discuss the issues associated with this force. What are the reforms required in this regard? (150 words) 10

Approach:

- Introduce by highlighting the role of the National Security Guard.
- Discuss the issues faced by this force.
- Mention the reforms required for the force.
- Conclude on the basis of above points.

Answer:

The National Security Guard (NSG) was raised in **1984** and institutionalised under the National Security Guard Act, 1986. It operates under the **Ministry of Home Affairs**. It is considered **India's premier counter-terrorist force** for anti-hijacking, counter-terrorism, hostage rescue and other such special operations. However, the handling of the 26/11 Mumbai attacks and the attack on Pathankot air base raised **serious questions about the preparedness** of these forces.

The **various issues** associated with this force are as follows:

- The NSG Headquarters and the Academy are **manned by a mix of personnel** from all the forces with different cultural and professional outlooks leading to **coordination challenges**.
- The organisation **is headed by Director General belonging to the IPS with limited practical experience** in handling counter-terror or irregular warfare operations.
- The forces are **stationed at only a few centres** across the country. Also, **NSG's limited independent logistics** capacity causes delay in reaching its destination. For instance, delay in arrival in November 2008 Mumbai attacks, from their base in Manesar, Haryana.
- Despite constantly redesigning training programmes, it still remains **inward looking with no new ideas in operational tactics.** For instance, lack of terrain information to NSG in different geographies led to delay in conclusion of operation in Pathankot Attack.
- The force continues to be marred by **shortage of cutting-edge equipment and training aids**. The proposed Rs.1400 crores modernisation plan has remained on paper.

A **range of reforms** have been suggested in this regard, such as:

- The forces need to be established as an **independent special operations command** with its own cadre and leadership.
- It should have a dedicated **Air Wing** to strengthen its aviation capability and timely movement.
- It should have **local quick response groups** (NSG hubs) under the central forces for rapid action response.
- There is a need to implement the **modernisation programme to effectively provide modern equipment** such as real time sensor shoot grid, vision and thermal image fusion cameras, and state of the art weaponry. The procurement system should be free from bureaucratic delays.
- **Training needs to be upgraded by sharing experiences** and interacting with specialist forces from other countries like the SAS (UK), GSG-9 (Germany).

Recently, the government has decided to remove NSG commandos from **VIP** security duties and also **proposed** a **NSG hub** in Punjab. In the wake of growing terrorist violence in different forms, it is pivotal that NSG emerges as a lean and agile force with focus on speed, stealth, precision and zero error.

8. Highlighting the key changes made by the National Investigation Agency (Amendment) Act, 2019, discuss the objections that have been raised against these. (150 words) 10

Approach:

- Give a brief account on the NIA Act.
- Enumerate the amendments made in the Act.
- Discuss the objections that have been raised against the amendments.
- Conclude on the basis of the above points.

Answer:

National Investigation Agency (NIA) is a central agency to combat terrorism in India, established under the **National Investigation Act, 2008**. It has wide powers such as, to take *suo motu* cognisance of terror activities in any part of India and register a case, to enter any state without permission from the state government, and to investigate and arrest people.

The **NIA (Amendment) Bill, 2019** was passed by the Parliament amending the original Act of 2008. Following are the amendments made:

- It **expanded the type of offences that the NIA could investigate and prosecute.** It can now investigate offences related to human trafficking, counterfeit currency, manufacture or sale of prohibited arms, cyber-terrorism, and offences under the Explosive Substances Act, 1908.
- The NIA will have the **power to investigate scheduled offences committed outside India**, subject to international treaties and domestic laws of other countries. A special court will preside over such cases.
- The amendment enables the **central government to designate session courts as special courts for NIA trials** under Section 11 and 22 of the NIA Act 2008.

However, the following **objections** have been raised against the recent amendments:

- The **new amendment has diluted the nature and operation of the Act,** which was enacted to prosecute offences affecting national security, by incorporating offences such as trafficking of minors for sexual exploitation etc., which **may not be related to terrorism**.
- The **expanded scope** of scheduled offences may be prone to **misuse by government,** which can categorize them as acts of terrorism. This is especially dangerous when the terms/ phrases like **'terrorism'**, **'affecting the interest of India'** have not been **defined** under the Act, which may be interpreted to **curb dissent**.
- The expanded jurisdiction covers matters (such as offences under the Explosives Act) which are also in the domain of the state governments leading to possible **encroachment on their jurisdiction.**
- The provision to designate the existing Sessions Courts as Special Courts will dilute the **exclusivity** of the NIA Act. These sessions courts would run on similar lines as they do under other Central Acts, thus **eroding the special character** of this Act. Also, these courts are **already overburdened with pending cases** and this move will further increase their burden.
- The power to investigate cases outside India would not be useful **without any cooperation and extradition treaties with other countries.**

The amendments have been brought to strengthen the National Investigation Agency. However, the aforementioned concerns need to be addressed so that there is a coordinated effort for the fight against terrorism.

9. Subsequent to the 26/11 Mumbai attacks, the coastal security arrangement has been thoroughly reviewed by the Government of India. Comment. (150 words) 10

Approach:

- Briefly mention the vulnerability of India's coastal borders and its failure to prevent the 26/11 attack.
- Highlight the changes/reforms made in the coastal security arrangement by the Government of India.
- Conclude on the basis of above points.

Answer:

The 26/11 Mumbai attacks exposed the vulnerabilities faced by India from the sea and its inept handling of coastal security matters including lack of coordination among different agencies. India continues to face **three levels** of **asymmetric threats** emanating from its long coastal borders:

- **Terror attacks** by non-state actors on population centres and vital installations like atomic power plants and naval guard bases.
- Threats posed by **organised gangs** carrying out smuggling of narcotics, arms and explosives as seen in the 1993 Mumbai Bomb blasts.
- Vulnerability of the Indian coast to **illegal inflow of migrants and refugees**.

The 26/11 attacks prompted a **paradigm shift towards a multi-pronged approach** in the maritime security apparatus with increased emphasis on surveillance, intelligence gathering and information sharing amongst the various stakeholders to ensure an effective response to any emerging situation.

Coastal Security Arrangement post 26/11 Mumbai attacks:

- **National Committee for Strengthening Maritime and Coastal Security** (NCSMCS): It is apex national-level review forum for maritime and coastal security, in which all concerned ministries and government agencies are represented.
- **Coastal Security Scheme (CSS):** It provides for a **multi-tier arrangement** for patrolling and surveillance, with the *Indian Navy,* the *Indian Coast Guard* and the *State Coastal Police*, jointly securing the Indian coasts in their respective jurisdictions.
- **Joint Operations Centres (JOCs**): They were set up by the Navy as **command and control hubs** for coastal security at Mumbai, Visakhapatnam, Kochi and Port Blair. They are manned 24×7 jointly by the Indian Navy, Indian Coast Guard and Marine Police.
- **Electronic surveillance mechanism** has been augmented by provisioning of a radar chain called **Coastal Surveillance Network (CSN)** consisting of, Chain of Static Sensors, Automatic Identification System (AIS), Long Range Identification and Tracking (LRIT), day/night cameras etc.
- **National Command Control Communication and Intelligence Network (NC3I):** This overarching coastal security network collates data about all ships, dhows, fishing boats and all other vessels operating near our coast, from multiple technical sources including the AIS and radar chain.
- **Fishing communities** have been made the **'eyes and ears'** of India's security architecture. It includes **coastal security awareness campaigns**, issuing **ID cards** to all fishermen with a **single centralised database**, registering and equipping **fishing vessels** with equipment to facilitate their **identification** and **tracking**.

Thus since 2008, coastal security arrangement has been strengthened substantially by these initiatives. Further, the coastal security exercises like the **Sagar Kavach** and recent pan India mega exercise **Sea Vigil** should be institutionalised.

10. Non-state actors are significant conduits in many important national security challenges faced by India. Explain with examples. (150 words) 10

Approach:

- Define non-state actors with their types.
- Give evidences for non-state actors posing a risk to national security challenges.
- Conclude on the basis of above points.

Answer:

Non-state actors are individuals or organizations that are **neither affiliated to nor controlled by** any particular state. These include insurgent groups, terrorist groups, drug cartels, mafias, non-governmental organisations among others.

Some non-state actors have **adversely impacted national security** of India by having an ability to aggravate already existing threats to India's national security in following ways-

- **Terrorist organisations** like Lashkar-e-Taiba and Jaish-e-Mohammad have conducted **multiple terror attacks** on India including the Parliament attack, 26/11 Mumbai attacks and the recent attacks on Indian army in Uri and Pathankot respectively in 2016. Apart from **stalling the bilateral dialogue,** such attacks often bring **two nuclear armed neighbours on the brink of an armed conflict**.
- Kargil conflict was triggered by **insurgent irregulars** in conjunction with the Pakistan army challenging India's sovereignty. The use of non-state actors allowed Pakistan **plausible deniability** on its involvement in the conflict. Also, while India had to use **expensive air and ground campaign**, Pakistan was saved from this cost of warfare due the use of these non-state actors.
- **Over-ground workers** (OGWs) of various anti-national organisations indulge in **spreading propaganda, arranging funds, recruiting new members, providing logistic support to strike teams, gathering intelligence** etc. These workers help sustain various movements like naxalism, terrorism, secessionism, insurgency etc.
- The Intelligence Bureau also suggested that **various NGOs** like Cordaid, Amnesty International etc. were **sponsoring agitations** against nuclear and coal-fired power plants across the country.
- **Organised criminals** indulge in various activities like drug smuggling, human trafficking, spreading counterfeit currency, gun running and other subversive activities. For example- D-company launched the 1993 Mumbai blast with a plant to cause communal riots all over the country.
- **India's maritime security** also faces threat by pirates (e.g. Somali pirates in Indian Ocean) and underwater attacks compromising critical infrastructure such as, the communication networks.
- India faces a high risk to its **critical information infrastructure** by **hackers' groups** from around the globe by way of **cyber terrorism**, **cyber-frauds**, **data theft** etc. For example- details of 32 lakhs debit cards of SBI were stolen in recent years and Pakistani hackers often target government websites in India.

India has taken various steps such National Intelligence Grid (**NATGRID**), Crime and Criminal Tracking Network and Systems (**CCTNS**), SAMADHAN, coastal defence exercise **Sea Vigil** etc. to curb such threats. Further, India needs to work towards focused operations, based on proper assessment and intelligence sharing to rein in non-state actors.

11. Incidents of naxal violence and its resultant deaths have been reducing consistently in the past few years. In this context, give an account of the multi-pronged approach that has been followed by the central and state governments for combating naxalism. (250 words) 15

Approach:

- Introduce by giving some arguments/data to support the reduction in naxal violence.
- Discuss the main areas of multi-pronged approach taken by the governments.
- Conclude on the basis of above points.

Answer:

As per the annual report of Union Ministry of Home Affairs (MHA), incidents of naxal violence have dropped by nearly 27% and its resultant deaths have reduced by nearly 40% in the five-year period from 2013 to 2018.

Government has been implementing National Policy and Action Plan (NPAP) incorporating multiple approaches to combat Left Wing Extremism (LWE). In most of the areas, both the central and state governments are working in tandem with each other.

Multi-pronged approach taken by Central and state governments includes the following:

- **Security Related Measures:**
  - **Institutional measures:** Specialised anti-naxal forces like Black Panther, Bastariya Battalion etc. have been established along with multi-disciplinary groups of officers from various agencies- IB, NIA, CBI, ED, state police etc.

- **Security Related Expenditure (SRE) Scheme**: Under the Scheme, the central government reimburses Security Related Expenditure relating to different requirements of state governments.
- **Special Central Assistance (SCA)** for most affected districts which have the main objective of filling the critical gaps in Public Infrastructure and Services, which are of emergent nature.
- **Assistance to LWE affected States** by providing CAPFs, UAVs, construction of fortified police stations, funds for modernization of State Police forces, sharing of intelligence etc.

- **Development Related Initiatives**
  - **Infrastructure Development:** Various ministries are implementing separate schemes such as Road Connectivity Project, Universal Service Obligation Fund (USOF) supported scheme to provide mobile services in LWE-affected states.
  - **Skill development related measures:** ROSHNI under DDU Grameen Kaushal Yojana for training and placement of rural poor youth and establishing ITIs and Skill Development Centres in naxal affected areas.
  - **Constructively engaging youth through education:** Seeing the success of educational hubs and a livelihood centre in Dantewada district, the government has now opened up livelihood centres, known as Livelihood Colleges, in all such districts.
  - **Other measures:** for development like more bank branches have been opened to ensure financial inclusion.
- **Confidence Building Measures aimed at winning hearts and minds:**
  - **Civic Action Programme (CAP)**: It has been implemented since 2010-11 to bridge the gaps between Security Forces and local people through personal interaction and bring the human face of forces before the local population.
  - **Surrender and rehabilitation policies:** Eligible surrenderees are imparted training in a trade/vocation of their liking and befitting their attitude with a monthly stipend for a maximum period of 36 months.
- **Media Plan Scheme:** It has been launched to counter the Maoist propaganda of misguiding and luring the innocent tribal/ local population by their so-called poor-friendly revolution.

This multi-pronged approach by the government addresses the various causative factors that lead to naxalism and insurgency. This, along with other factors like loss of cadres/leaders on account of arrests, surrender and desertions, insurgency fatigue among the maoist cadres, choking of funding through PMLA etc. have reduced naxal violence and its resultant deaths. To further eliminate the problem, government has now initiated a new doctrine – **SAMADHAN**, a multi-pronged strategy to frame short term and long-term policies to tackle naxalism.

12. With increasing incidents of cyber attacks, it is imperative that India takes urgent steps to address the cyber security challenges that it currently faces. Discuss. (250 words) 15

Approach:

- Introduce by highlighting the increasing incidents of cyber-attacks and cyber crimes.
- Explain the challenges faced vis-à-vis cyber security in India and steps taken briefly.
- Mention the steps needed to be taken to address these challenges.

Answer:

According to the Data Security Council of India (DSCI), India has been the second most cyber-attacks' affected country between 2016 and 2018. These increasing incidents are due to multiple cyber security challenges:

- **Widespread digital illiteracy:** It makes Indian citizens highly susceptible to cyber fraud, cyber theft, etc.
- **Using substandard devices:** In India, the majority of devices used to access the internet have inadequate security features. Also, they do not meet appropriate security standards.
- **Import dependence** for the majority of electronic devices from cell phones to equipment used in the 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.
- **Sophisticated nature of attacks**: Though phishing is a generally well-known attack, hackers and malicious actors are becoming smarter due to technological evolution, and their attacks are becoming more and more sophisticated as shown by the Wannacry and Petya ransomware.
- **Lack of coordination**: In India, critical infrastructure is owned by both public sector and private sector, both operating with their own norms and protocols for protecting their infrastructure from cyber-attacks. The armed forces too have their own agencies for it. Private sector, despite being a major stakeholder in cyberspace, has not been involved proactively for consultation and development of cybersecurity architecture in India.

To tackle these, the government has taken steps such as formation of National Cyber Coordination Centre (NCCC), Indian Computer Emergency Response Team (CERT-In), National Cyber Security Policy 2013 etc. Recently, Indian Cyber Crime Coordination Centre (I4C) was set up to deal with all types of cybercrimes in a comprehensive and coordinated manner. In addition, India needs to undertake the following **steps** to address the aforementioned challenges:

- **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.
- **Cyber-attack deterrence:** 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.
- **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 that penalties serve as deterrence for crimes. For example, in the Indian IT Act, financial fraud is still a bailable offence.
- **Become part of international conventions and adopting international standards:** India should consider signing of the Budapest Convention on cybercrime to garner global support. Also, adhering to international standards must be made applicable for all government websites, applications before hosting and publishing.
- **Establishing cybersecurity framework at state level:** For example, establishment of state CERT to work in conjunction with CERT-In.

The government of India plans to launch a National Cyber Security Strategy, which would deal with all issues related to cyber security including standardization, testing, auditing and capacity development.

13. Identify the various issues related to Indo-Bangladesh border and challenges faced in managing this border. What measures has the government taken in this regard?

(250 words) 15

Approach:

- Giving a brief introduction, identify issues related to the Indo-Bangladesh Border.
- Then discuss challenges that are being faced in managing the border.
- Then bring out the measures that have been taken by the government in this regard.
- Conclude accordingly.

Answer:

India shares the longest land border with Bangladesh, stretching over 4097 km, which runs through a diverse topography.

The **issues related to the Indo-Bangladesh border include:**

- **Illegal immigration:** Since 1971 War, illegal immigrants have been pouring into India. They act as a security risk and a social economic threat to the natives.

- **Criminal activities across the border:** Transnational crime networks smuggle narcotics, arms, gold and counterfeit Indian currency and are also involved in trafficking of humans, cattle and goods.
- **Movements of insurgents across the border to safe havens in Bangladesh:** The North-eastern outfits in India such as ULFA, NDFB, DHD etc. are alleged to have had safe havens in Bangladesh.
- **Cross-border water disputes:** Such as sharing of Teesta River, construction of dam by India on Barak River has plagued the border management and bilateral relations.

Challenges faced in managing Indo-Bangladesh Border:

- **Topography:** The dense forests, hills and rivers in the border region make it's patrolling very difficult. Withdrawal of the forces for other duties (counter-insurgency operations, election work for prolonged period), further worsens the problem.
- **Difficulty in identifying Bangladeshi nationals:** It is difficult to identify an illegal Bangladeshi migrant in the absence of identity cards in the border areas. There has been alleged connivance of the locals with infiltrating Bangladeshis, which makes the task of detection more difficult.
- **Overpopulated border areas**: Density of population at some places is approximately 700-800 persons per square km on the India side and about 1000 persons on the Bangladesh side. Such an overpopulated area along with a porous border poses severe security challenges.
- **Ethnic conflicts and separatist movements:** Changing demographic profile of many border-states due to illegal migration is giving rise to ethnic conflicts, such as in the state of Assam.
- Other challenges include understaffed and overworked security forces, cross border cooperation among militant groups etc.

Measures taken so far in this regard are:

- **Maritime border dispute resolution**: Resolution of Bay of Bengal maritime boundary arbitration between Bangladesh and India over the New Moore or South Talpatti island in 2014 led by Permanent Court of Arbitration (PCA).
- **India Bangladesh Land Boundary Agreement, 2015**: It facilitated exchange of enclaves and simplified border management.
- **Improved border surveillance:** through **CIBMS**, also known as smart fencing has been completed in some parts of the border. Project BOLD-QIT has been implemented along the riverine border in Dhubri, Assam.
- **Coordination with border states:** Central Government has announced setting up of Border Projection Grid with Indo-Bangladesh Border states, which will be supervised by a state level standing committee to be chaired by respective state secretaries.
- **Improved border management:** So far 20 border checkpoints have been developed as Integrated Check Posts and joint military training exercise 'Sampriti' has been conducted since 2010.
- **Confidence building measures:** Government to government initiatives to promote local participation such as border haats have shifted focus to mutual economic gains and building a coalition for peace and cooperation.

These measures have started showing results as, according to the data provided by the government, the detected infiltration through the India-Bangladesh border has dropped by over 60 per cent since 2015.

14. In context of challenges faced by India due to terrorism, it is important to identify and address terror-organized crime nexus and it's financing through drug trafficking. Discuss.

(250 words) 15

Approach:

- Introduce the answer with terrorism-organised crime nexus and its financing means.
- Explain the importance of addressing terror-organized crime nexus and it's financing through drug trafficking.

- Discuss the measures needed to tackle the menace of terror-organised crime funded via drug trafficking.
- Conclude the answer.

Answer:

Terrorism in India affects multiple lives and disrupts several families each year. It affects India's socio-economic development and poses serious risk to the critical infrastructure as well as the overall stability of the country. Criminal groups join hands with terrorists to provide illicit financing through drug trafficking, arms dealing, money laundering and counterfeiting. Depending upon the circumstances, these groups can coexist, cooperate and even converge.

It is important to identify and address terror-organized crime nexus and it's financing through drug trafficking due to the challenges it poses, such as:

- In India and its neighborhood, several examples of drug trafficking financing terror-networks, can be traced. For example, of an estimated USD 29 million generated in 'illegal taxation' of opium revenues in Afghanistan in 2018, USD 21 million was said to be collected by anti-government elements, including the Taliban. **Cross-border nature of such fused entities and their financing activities** pose a serious challenge to India and coordinated international response is too slow to be effective in most cases.
- Mobilisation activities of UN-designated terrorist organisations such as ISIL, Al-Shabab, Al-Qaida, Boko Haram, Lashkar-e-Taiba and Jaish-e-Mohammed **destabilise entire regions through cross-border financing, propaganda, and recruitment**, by exploiting global public goods such as the cyberspace and social media.
- Drug trafficking has provided **funding for insurgency** and those who use violence in various regions throughout the world, including in transit regions. In some cases, drugs have even been the currency used in the commission of terrorist attacks, as was the case in the Madrid bombings (2004).
- The world drug problem now includes **new substances, synthetics, new technology used to market drugs, encrypted communications, AI, virtual currencies** which are transacted making the entire ecosystem highly profitable and difficult to track.

Terrorists activities and operations cost money, so understanding how groups raise, store, move, and spend that money helps bring terrorists to justice and deters others from harboring them or funding or joining their organizations. In order to mitigate the impact of the menace of terror-organized crime funded via drug trafficking there is an emergent need to undertake the **following measures:**

- **International coordination**: The UN needs to increase cooperation with bodies such as Financial Action Task Force (FATF), which is playing a significant role in setting global standards for preventing and combating money laundering and terrorist financing.
    - Real-time intelligence sharing and capacity building would go a long way to fight terror financing via drug trafficking.
    - Cooperation in the analysis of crimes related to illicit narcotic-trafficking and harmonization of national legislation is another requirement.
- **Regional measures**: Such as the SCO's Regional Anti-Terrorist Structure (RATS) and its coordination with UNODC should be undertaken by various groupings such as SAARC.
- Measures to **tackle cyber-terrorism** must be undertaken to minimize the impact of terror-financing.
    - Efforts centered on countering money laundering and terrorist financing, cybercrime, as well as trafficking in firearms, drugs and cultural heritage must be incorporated.

The terror-crime nexus and related drug-financing is an existential global threat, the contours of which are mutating every day. To combat this menace, we need to keep ahead of the new trends and technologies, something that can only be achieved if all countries work together, with a zero-tolerance approach.

15. What are the social, economic and political costs of money laundering? Highlighting the necessity of trans-national cooperation for its prevention, enumerate various initiatives taken by the international community. (250 words) 15

Approach:

- Give a brief introduction of money laundering.
- Mention the social, economic and political costs of money laundering.
- Highlight the need for trans-national cooperation for its prevention.
- Enumerate various initiatives taken by the global community.

Answer:

Money laundering is the process of making **money** generated by a criminal activity, such as drug trafficking or terrorist funding, appear to have come from a legitimate source. It is a multi-stage process accomplished through various methods like structuring deposits, shell companies, third party cheques, bulk cash smuggling etc.

The costs of money laundering, if left unchecked or dealt with ineffectively, are serious. Organised crime can infiltrate various segments of an economy, which can have cascading effects on its social and political life as well.

Costs of money laundering

- **Economic**: Organised crime can infiltrate financial institutions; acquire control of large sectors of the economy through investment by this route. It can erode a nation's economy by changing the demand for cash, making interest and exchange rates more volatile etc. This poses damage to the reputation of financial institutions and the market of a nation and discourages foreign investment.
- **Political**: The offer of bribes to public officials by criminal organisations may lead to them gaining political influence, thereby undermining democratic processes and affecting policy decisions.
- **Social**: The economic and political influence of criminal organisations can weaken social fabric and collective ethical standards. Further, money laundering is inextricably linked to the underlying criminal activity that generated it and enables criminal activity to continue.

Necessity of trans-national cooperation

There is a need to enlist common predicate offences to solve the problem internationally particularly because of the trans-national character of the offence of money laundering. Trans-national cooperation is required to ensure:

- **Convergence among various agencies** of the world against the issue of money laundering, which is borderless. It would help them in not getting stuck in the different laws and procedures of their respective countries.
- **Harmonisation of efforts** against money laundering and build a consensus regarding common predicate offences keeping in mind the trans-national character of the offence.
- **Solving the issue of financial confidentiality,** which in the case of lack of cooperation, states are unwilling to compromise upon.

Initiatives taken by global community

- **Financial Action Task Force** (FATF): It is an inter-governmental body that sets standards and promotes effective implementation of legal, regulatory and operational measures to combat money laundering and terrorist financing and other related threats to the integrity of the international financial system.
- **Asia Pacific group**: It works with countries in the Asia-Pacific to generate wide regional commitment to implement anti-money laundering policies and initiatives and secure agreement to establish a more permanent regional anti-money laundering body.
- **Basel Committee on Banking Regulations and Supervisory Practices** issued a statement of principles to ensure that banks are not used to hide or launder funds acquired through criminal activities.

- **Various international conventions** are also established to prevent money laundering such as the United Nation Convention against Transnational Organised Crime (2000) among others.
- **Tax treaties** that facilitate and enhance exchange of information under the Tax Treaties e.g. India's Foreign Account Tax Compliance Act with the US.
- **The Multilateral Competent Authority Agreement** (MCAA) is also developed for Automatic Exchange of Information as per Common Reporting Standards (CRS).

Money laundering involves large-scale activities that are also international in nature. Therefore, to make a heavy impact it is necessary that all countries should collaborate and enact strict and uniform laws, as far as possible.

16. Despite its obvious advantages, doubts have been raised regarding the ability of Comprehensive Integrated Border Management System (CIBMS) to secure India's key borders. Discuss. (250 words) 15

Approach:

- Give a brief introduction about the Comprehensive Integrated Border Management System (CIBMS).
- Enlist the advantages of the Comprehensive Integrated Border Management System (CIBMS).
- Mention the issues involved with the Comprehensive Integrated Border Management System (CIBMS).
- Conclude by giving a way forward.

Answer:

The Comprehensive Integrated Border Management System (CIBMS) is a robust and integrated system that is capable of addressing the gaps in the present system of border security. It aims at seamlessly integrating human resources, weapons, and high-tech surveillance equipment.

Technical solutions are necessary to augment and complement the traditional methods of border guarding. The CIBMS has the **following advantages**:

- Use of ***high-tech surveillance devices*** such as sensors, detectors, cameras, ground-based radar systems, micro-aerostats, lasers etc. that will help in **round-the-clock reconnaissance** of the international border even under different weather conditions.
- ***Communication networks*** including fibre optic cables and satellite communication will **help in transmitting data** gathered by these diverse high-tech surveillance and detection devices.
- ***Command and control centre*** will help by receiving the transmitted data and **providing a composite picture of the international border**.
- It would also help in **reducing the human error and stress level** among the border guarding personnel to a large extent.

The purpose of the CIBMS is to eventually replace manual surveillance of the international borders.

Despite these advantages, doubts have been raised regarding the ability of CIBMS to secure India's key borders because of the following **issues** that India might face:

- The system might suffer numerous **technical glitches** such as a large number of false alarms, line of sight constraints, unreliable information transmission, and equipment malfunction.
- At present, many of the high-tech surveillance devices deployed by the BSF are not optimally utilized because the required **technical expertise is not uniformly available** among the force's personnel.
- The **exorbitant cost of the electronic devices and the lack of easy availability** of spare parts act as a deterrent against their use.
- **Erratic power supply and adverse climatic and terrain conditions** in the border areas could potentially undermine the functioning of the sophisticated system.
- Helium-filled Aerostat balloons can provide an aerial 24/7 surveillance and communications, but they can also be easily targeted by cross border guards. Moreover, one time use or refilling

it is likely to cost approximately rupees one lakh, calling into question the financial sustainability of the project.

Technical solutions are necessary to complement the traditional methods of border guarding. However, caution must be exercised while advocating the use of high-tech and high-cost electronic devices for border security. The experiences of countries such as the United States that have employed high-tech devices demonstrate that not only are the costs of such devices prohibitive but that they also fail to provide a comprehensive solution to border security problems.

Instead of high-cost and innovative technological solutions that require extensive technical expertise, a **judicious mix of properly trained manpower and affordable and tested technology** is likely to yield better results.

17. Why is radicalisation seen as a significant security challenge for India? Suggest ways to tackle it. (250 words) 15

Approach:

- Briefly discuss what is radicalisation in introduction.
- Discuss why radicalisation is seen as a security challenge for India?
- Suggest ways in which India can tackle the problem of radicalisation.
- Conclude accordingly.

Answer:

Radicalisation is a process with multiple reinforcing pathways of developing extremist beliefs, emotions, and behaviours. Whether based on religious, ethnic or political grounds, extremist ideologies glorify the supremacy of a particular group or cause, and motivate people to use violent means against members of an out-group or in pursuit of the cause.

Radicalisation is seen as a significant security challenge for India due to various reasons:

- Radicalisation is the **first step towards violent extremism,** which in turn may lead to loss of human lives. It has the potential to **tear apart the social fabric** and increase the probability of a polarised society in such a diverse country as India.
- It is **used by the enemy countries or extremist organisations to instigate resentment** amongst the people by taking advantage of the factors like lack of economic development, mis-governance etc. In India, it is spread over many parts of the country - Jammu Kashmir, North Eastern States, Punjab etc. Moreover, radicalisation has also created problems in the South Asian region, which is India's neighbourhood
- Further, with the **rising number of social media users** in India, the threat of internet-facilitated indoctrination becomes imminent as it may lead to rapid increase in recruitment by militant agencies through social media. The Islamic State and other such organisations have indeed used this path. This along with the trend of **reasonably well educated and urban youth** joining militant organisations makes it a prominent security concern.
- As radicalisation is fueled by an ideology, unlike other, more physical manifestations of violence, radicalization cannot be countered by traditional kinetic measures only.

Although India is taking steps like setting up de-radicalisation camps, roping in scholars of ideological or religious affiliation for counselling etc., there are some steps that the government can take to tackle the problem of radicalisation:

- **Developing a comprehensive policy framework** that focuses on de-radicalisation and works in tandem with the peculiarities of each state.
- **Roping in senior citizens and family members** to share their words of wisdom with vulnerable youth and monitor suspicious online activities of children and help bring them back into the mainstream.
- **Building counter-narratives on social media** that would help in tackling social media propaganda originating from other countries as well as from extremist organisations. The government must launch both online and offline campaigns targeting the right audience along

with an effective content-based online regulation, blocking of websites and removing extremist propaganda.

- **Training officials and staff members** of the agencies working in counter-radicalisation in matters related to special aspects of different communities' religious and cultural sensibilities and the way investigations against extremism should be conducted.
- **Undertaking efforts towards de-radicalisation and rehabilitation** of the detainees charged with crimes of violent extremism.
- **Developing close cooperation with other countries** in conducting counter-radicalisation programmes including integration and dissemination of information.

The problem of radicalisation has seen an uptrend. There is a need to avoid discrimination between one kind of radicalisation and another. Strengthening social resilience is an important tool in countering radicalisation in all its forms, targeting all types of people. Thus, it is important to conduct meaningful research towards development of a counter-radicalisation framework, which is both preventive and curative in nature and also rehabilitates the misguided youth of the nation.

18. Identify the opportunities and challenges that social media presents to the law enforcement agencies in India to counter national security threats. What steps have been taken to address the challenges? (250 words) 15

Approach:

- Provide a brief introduction of social media usage in India.
- Mention opportunities and challenges posed by it to the law enforcement agencies in countering national security threats.
- Mention steps taken by the government to address these challenges.
- Conclude with a way forward.

Answer:

With over 500 million active Internet users, social media usage in India is also on the rise. In this context, factors such as increasing internet penetration, young demography, digital initiatives and local language computing are projected to throw several opportunities and challenges to the law enforcement agencies in countering national security threats.

Opportunities:

- **Increased engagement with citizens**: The social media enables increased engagement with citizens to build secure communities, which share information that may be used to support investigations.
- **Improved intelligence capabilities:** It offers real-time, first-hand information, which can be used for developing "actionable intelligence" regarding possible flash points of disturbances by using tools such as big data analysis etc. and sharing across agencies.
- **Enhanced preparedness**: It may also be used to prevent misuse of social platforms to spread malicious rumours, which may trigger problems for internal security and law and order, and prepare standard operating procedures for times of emergency.

Challenges:

- **Increased number of cyber-crimes:** Criminals are using social media for sale of contraband items, selection of targets and victims, spreading malware, committing cyber frauds, impersonation, hacking etc. For example, recently, Pakistan has been found 'honey trapping' Indian soldiers, scientists etc.
- **Unregulated space for propaganda:** Terrorists and extremists are using social media to propagate their ideology and recruit members. For example, radicalisation done by ISIS and use of tremendous online following by Burhan Wani to strengthen Hizbul Mujahideen in Kashmir Valley.
- **Fast paced spread of misinformation**: Foreign entities are using social media as a weapon in their psychological operations to cause unimaginable disruptions. For e.g. Pakistan's ISI

uploaded fake inflammatory videos, which triggered exodus of people from North-eastern India staying in Bangalore and Pune.

- **Ineffective laws:** The Indian legal framework that includes IT Act, 2000 and National Cyber Security Policy, 2013 is both inadequate and face limitations in present circumstances. For e.g. denial by WhatsApp to help trace the origin of posts which led to lynching of 5 men in Maharashtra.
- **Democratic rights:** It is also difficult for India to strictly regulate the social media because freedom of speech and privacy are fundamental rights.

Steps taken by India:

- **NETRA (NETwork TRaffic Analysis):** This software has been developed by DRDO in 2014 and is being used by IB and R&AW for real-time detection of suspicious "keywords" and "keyphrases" in social media, emails, blogs, tweets, instant messaging services, and in other types of Internet content.
- **Social Media Labs**: They are used to detect suspicious activity, and track mobilisation using social media for protests, and support domestic law enforcement.
- **Crime and Criminal Tracking Network System (CCTNS):** Launched in 2009, one of the stated goals of CCTNS is **predictive policing** i.e. real time tracking of internet data including social media data, for domestic law enforcement.

The Government of India is planning to bring comprehensive Social media Regulations and a National Cyber Security Strategy by 2020. A National Media Analytics Centre (NMAC) has also been proposed by the National Security Council.

19. It is widely recognised that India's Central Armed Police Forces (CAPF) are in urgent need of overhaul. Discuss in the context of issues associated with personnel, infrastructure and service conditions of these forces. (250 words) 15

Approach:

- Briefly explain what you understand by CAPF forces.
- Discuss the issues and challenges faced by CAPF forces in terms of personnel, infrastructure and service conditions, which need overhaul.
- Conclude appropriately.

Answer:

The Central Armed Police Forces (CAPF) refers to uniform nomenclature of seven security forces in India - Border Security Force (BSF), Central Reserve Police Force (CRPF), Central Industrial Security Force (CISF), Indo-Tibetan Border Police (ITBP), Sashastra Seema Bal (SSB), Assam Rifles and National Security Guard (NSG). They come under the Ministry of Home Affairs and perform various functions such as guarding of borders, security of sensitive establishments, counter terrorism and counter-naxal operations.

In the recent past their importance has increased due to **increased deployment and dependence of states** on them. This has also brought to light several issues being faced by these forces, which need to be addressed:

- **Personnel:**
  - There is **high attrition** in the CAPF mostly due to unregulated deployment of personnel and job discontentment. The number of personnel opting for voluntary retirement schemes in the CAPF rose to around 450% in 2016-17 as compared to the previous year according to the Home Ministry.
  - There is a **lack of promotional avenues** for CAPF personnel as IPS officers enjoy a de-facto monopoly on the leadership of the forces despite having limited experience of leading them.
  - They face **discrimination with regard to pay parity** in comparison with their counterparts in the armed forces and 'Group A Organised Services'. It was only recently that the CAPF personnel were granted 'non-functional upgradation', which is given to 'Group A Organised Services'.

- **Infrastructure:**
  - There is a **lack of effective arms and ammunition** such as bullet-proof jackets, modern arms, surveillance equipment, armoured vehicles etc. There is also **haphazard expansion of CAPF forces**, which adds to the infrastructural burden.
  - **Budget outlays** allocated for capacity augmentation of the CAPF are inadequate. Further, the **procurement process** under the 'Modernization Plan' of the CAPF is cumbersome and time consuming.
  - There is a need to **upgrade the curriculum and infrastructure** in CAPF training institutes. Further, the personnel need to be adequately trained in emerging threats such as cyber security.
- **Service conditions:**
  - According to the NCRB data, as many as 2,200 CAPF personnel died in accidents and suicides from 2014-2018. The Ministry of Home Affairs has revealed that suicides are mostly committed due to reasons such as **lack of stability, loneliness and domestic strife.**
  - The forces are burdened due to **indifference of superiors, lack of timely sanctioned leave and basic medical facilities**. Further, they **work in harsh conditions** without any standard rotation policy. For instance, the ITBP personnel are posted in snow-bound areas all year round.
  - There is **absence of in-house grievance redressal mechanism**, due to which personnel take to social media to complain about poor housing and working conditions.
  - **Continuous deployment** leaves less time for rest and recuperation and adds to their frustration. The deployment of CAPF's battalions has increased from 91 in 2012-13 to 119 times in 2016-17.

India's CAPFs play a very important ground role in India's national security. They require a serious overhauling across spheres like resource allocation, accountability structure and personnel management. These challenges must be adequately addressed and independent bodies should periodically review their service conditions and other grievances.

20. The ongoing Covid-19 pandemic has expanded and rearranged the concept of national security, making it more inclusive, and foregrounded human security in a more holistic manner. Comment. (250 words) 15

Approach:

- Discuss the erstwhile notions around global security and its heavy reliance on hard security.
- Discuss the ways in which Covid-19 pandemic has broken and reshaped the concept of nation and human security.
- Conclude with what needs to be done to make the concept of national security more inclusive and foregrounded human security in a more holistic manner.

Answer:

The concept of security that evolved in the 20th century was dominated by military considerations and territoriality. The post war conception of security largely prioritized hard security with emphasis on military aspects. The epidemic/pandemic threat and its impact on human security was seen as non-traditional security issue. It was not given much importance and seen as a relatively lower policy priority by way of funding and capacity-building.

However, the widespread and unprecedented impact of Covid-19 has in a way expanded and rearranged the concept of security. Its global expanse and tragic effect on human life has redefined both national and human security:

- The pandemic has disturbed the international system driven by increased global connectivity and physical mobility of people and goods. It has introduced an element of **unpredictability** specifically in relation to unimpeded **supply chains of essential goods & services.** For e.g. prescription drugs, oil etc.
- There have been marked **strains on otherwise tight alliances** for instance refusal to send critical supplies to Italy by otherwise less affected members of the EU.

- The dominance of **military considerations seem to** have taken a backseat briefly as many in the armed forces have also succumbed to the infection. E.g sailors aboard the USS Theodore Roosevelt testing positive for Covid-19
- It has revitalised Gorbachev's **'indivisibility' doctrine** in context of security, i.e. security is indivisible for there could be either equal security for all or none at all.
- National security is now being conceptualised in an **inclusive manner**, forging nations with varied military and ideological leanings into a collective. The Indian initiative to initiate a summit-level South Asian Association for Regional Cooperation (SAARC) consultative process is a prime example.
- Emphasis is now being laid over the **centrality of human security** in the national security template. The complete lockdown will create an economic crisis and misery for the poor with massive job losses and rising food insecurity may lead to newer basis of conflict.
- The **multi-layered and graded nature of human security** is being acknowledged, i.e. its dependence on a variety of factors, including individual genetic pedigree, socioeconomic indicators, nutrition levels and the local ecosystem.

Aftermath of the COVID 19, pandemic will provide the platform for rethinking the concept of national security that could be more inclusive with taking **health security** as a component of national security. Apart from that**, food security, wage security, shelter, education, tackling of fake news and information, upholding feelings of public safety, tackling public anxiety and panic** during such situations should be taken into consideration for designing future national security architecture. Also, countries and humanity need to rethink their priority in terms of their budgetary allocations and future investments, which needs more humane consideration.