Internal Security

We need security from what?

- Threat
    - Internal
        - Ministry of Home Affairs responsibility to counter internal
        - Left Wing Extremism/ Naxalism → CPI(Marxist- Political and Maoist- Naxal)
    - External
        - Army as an institution to deal with external that is Ministry Of Defence (we cannot use army for internal issue because it will be bloat on democracy)
    - External Supporting Internal

Coordination is required between MoD and MHA

Difference between left and right

- Economic difference
- Cultural difference

Who is the extremist?

UAPA→ even the individual person can be tagged as a terrorist.

Porous borders and illegal migration are the threat.

Management of borders is the responsibility of which ministry?

- MHA and MoD
- LoC→ Indian Army
- Siachen→ Indian Army and Air force

A State can be addressed from 4 kind of threats

- Internal
    - Naxalism, violent insurgency
- External
- Internal aiding external
    - Terrorism
- External aiding internal

Internal security is a security of a country within its border that basically implies maintenance of peace, law and order and upholding the sovereignty of the country within its territory.

Internal security

In India it is the Ministry of Home Affairs and internal security comes under the purview of **Police** which can be supported by **Central Security Forces(**if required**)** while external security is a security against aggression via foreign country

Threads

- **Traditional threats-** it has been understood in relation to States sovereignty and its territorial integrity as expressed in Article 2 of UN charter. So traditionally security policies were concerned with preventing war.
    - A Distinct trend in international security in the post cold war era is the phenomenal rise in non traditional security threats which includes issues like terrorism, food and water security, climate change, epidemics, secessionist movement, religious intolerance, financial instabilities, cyber crimes, migration crisis.
- **Non-Traditional threats-** Terrorism

Concept of peace and democracy

- Peace is a social and political issue that ensures the development of the society and the country. It's a State of harmony characterized by the existence of healthy relationships between different groups in the society. It is also related to a working political order that serves the true interest for all. In the context of geopolitics peace is not merely the absence of war or conflict but also the presence of social cultural and economic understanding and unity. The Millennium development goal adopted by the United Nations in 2000 identified peace and security as the key conditions for the successful development. It also recognises that development, peace and security and democracy are interlinked and mutually reinforcing. Thus these concepts are inseparable combined together and it creates a condition where individual, regions, Nations and the world move ahead without any threat as democracy creates the conditions for the elimination of public dissatisfaction as democratic system provides equal opportunity to all to participate in the process of governance and decision making and development insurance that people should not suffer from any sense of deprivation which leads them indulge in protest and violent activity. Thus development ensures the stability and the security of the individual and nation.
- Peace precedes development

Mandate of Central Security Forces

- CAPF
    a. BSF- to manage the border Indo Pak and Indo Bangladesh
    b. CRPF- primary role of CRPF is to assist state and police in maintaining law and order and it also plays an important role in conducting elections across the country. Some specialised formation of CRPF are
        i. Rapid Action Force- communal sensitive area for riot control (specialisation-multi ethnic composition and better mobility for swift action and the role is to control communal riots)

ii. COBRA Battalion- to tackle naxalism and their personal trainer by army and it became operational in 2008. And cobra personnels are trained and equipped for operations especially against left wing extremism.
iii. Special Duty Group- it is an elite CRPF group because its member are trained in combating nuclear and biochemical attack and its task is to provide armed protection to the SPG protected places
iv. Parliament Duty Group- elite CRPF unit and are trained to combat against nuclear and biochemical attack and armed protection to the parliament of India. After parliament attack

c. ITBP- Tibet
d. CISF- in 2009 government of India authorised CISF to provide security cover to even private and cooperative establishments across the country for the fee. Eg:- Infosy- CISF.
e. SSB→ Nepal and Bhutan (open border)
f. NSG→ it is also under MHA and it is a 100% deputation post. All personnel are posted on deputation from army, Central security forces, state police organisation. And its primary task is to engage and neutralize terrorist threats.eg. operation Taj. (5 NSG hubs→ Mumbai Kolkata Hyderabad Chennai and Gurgaon) and there are also assigned the task of providing mobile protection
g. SPG→
h. RPF→ railway protection group. To protect the lifeline of India its property and property of passenger.
i. First to six are under ministry of home affairs
j. SPG is under cabinet secretariat (1st IAS)
k. RPG under ministry of railway
l. And all the services are headed by IPS officer

- Armed forces

- CPMF

Communal violence is first taken through presidential rule.

Paramilitary

- Closer to army force
- **Assam Rifles** is the first paramilitary force also known as the friends of northeast
- It is completely deployed in North East and its mandate is to perform dual role
    a. Internal security in North East that is counter insurgency operations
    b. And to guard Indo Myanmar border
- It is led by army officers but under the administrative control of MHA.

Terrorism

- The degree of ideology fluctuate the definition of terrorism and crime.
- Nonconformists are tagged as extremist by the majority.
- Violent extremism is termed as terrorist.
- All terrorists are extremist but extremists are not always terrorists.
- Nonviolent extremist are the reformers (example→ Gandhi by British)
- Ideology of violence determined crime and terror.

Terrorist Justification for violence?

Terrorism has the potential to push to nuclear States against each other.

Media is is acting as an unintended propaganda tool for terrorism

Terrorism has become a global phenomenon and it is a non traditional threat but all attempts in the past for arriving at an internationally accepted definition has proved futile. Terrorism may be defined as planned, organised and systematic use of violence against the state and the civilians for political, religious and ideological objectives.

The ambivalence to arrive at the objective definition of terrorism are due to these reasons

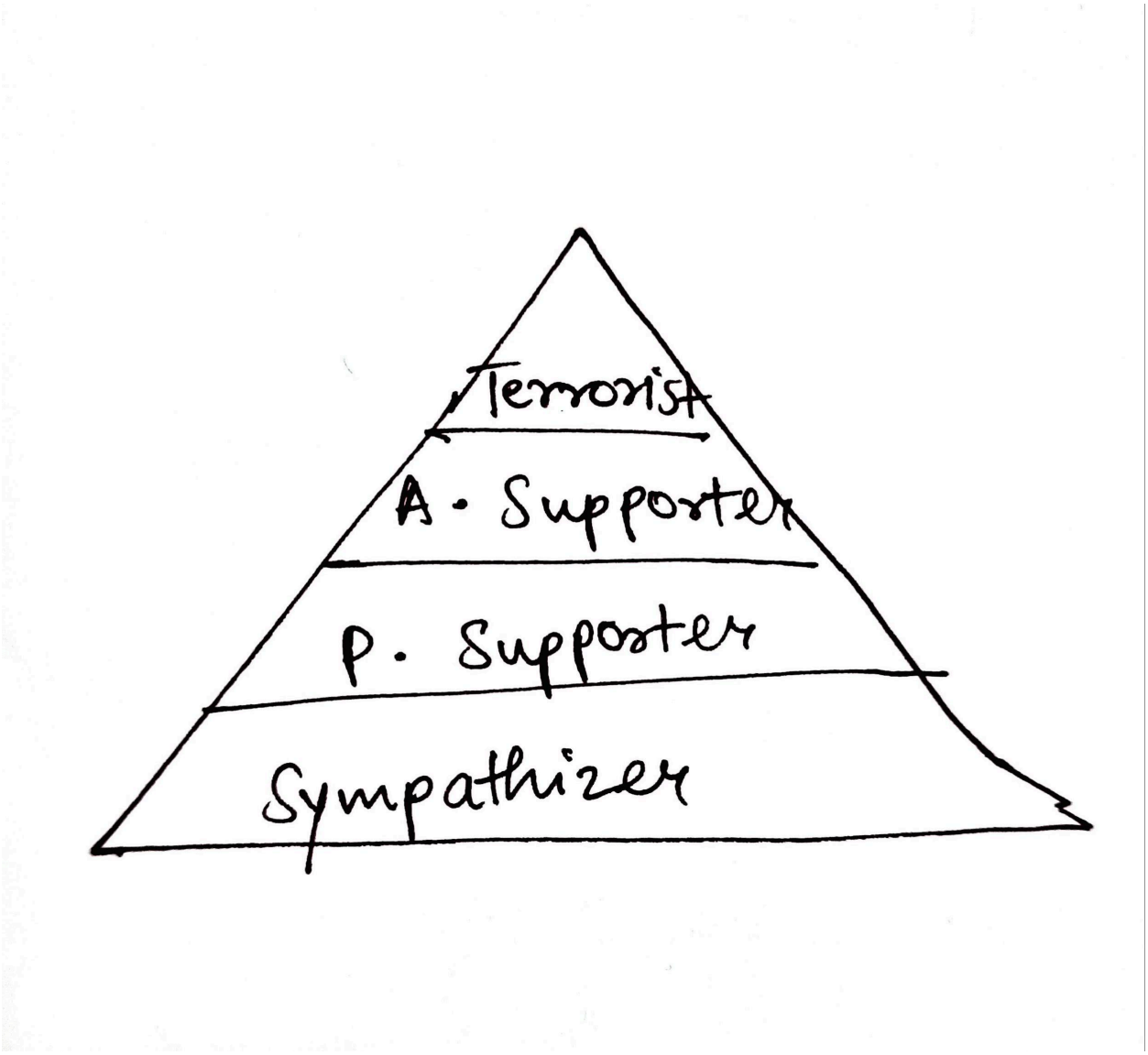
1. Terrorist in one country may be viewed as the freedom fighter in another
2. It is a well known fact that some states use violence against their civilians and support violence against the civilians of others states.

Thus due to the above two reasons there is an obvious lack of political will to have any universally accepted definition of terrorism.
Media is the communication channel through which news and other forms of data are shared.
The recent proliferation of mass media has resulted in the greater competition between the media groups for information that is believed to keep audience captivated, boost rating while increasing profits
The transfer from mainstream media to social media in the last decade or so had afforded the terrorist group the convenience, affordability and unfounded level of exposure to send their message worldwide.
The problem does not lie in that why media covers terrorism but how it covers it? As the selection of specific words can even portray favourably or unfavorably
Some of the positive connotations are freedom fighters, liberators, peacekeepers, nationalist.

While the negative connotations are

- Invaders, occupiers, terrorist

Media has emerged as an important tool for the terrorist organisation to propagate their ideology, to instill terror in the audience and to demonstrate their commitment and resolve and to continue their fight until their goal is achieved.



Rightist

- Economically capitalist
- Culturally they are conservative
- Right wing extremism is equal to the terrorism

Majority violence is called fascism and minority violence is called terrorism.

Leftist

Who is fundamentalist?

- Rigidity in the belief system is called fundamentalism.

Mob lynching and cow lynching are act of terror.

This support base is ruined in the presence of media and that's why media is being tagged as the unwilling ally of terrorism.
Existing researches have concluded that many terrorist attacks do not receive much attention from major media outlets unless the act involves a high amount of violence and this is affecting the future terrorist attack is there plan to kill the innocent more in order to gain publicity. Thus the ability to gain media exposure is not only increasing the number of attacks being traced and it has also resulted in increasing the severity of attack. Terrorist groups are carefully selecting the places to carry out their attack in order to get the best media coverage and this process of manipulation of media group by the terrorism has held to the criticism of media
However according to the media groups terrorism should not affect the importance of the freedom of expression as it is one of the essential foundation of democratic society and this freedom carries with it the right of the public to be informed on matters of public concern including terrorist attacks and threats as well as the responsible this state and the international organisation towards them. Thus according to the media group the war against terrorism should not be used as an excuse by the states to restrict the freedom of press as media is the fourth pillar of democracy.

Extreme Left→ naxal
Extreme right→ fascism

Factors that give rise to naxalism?

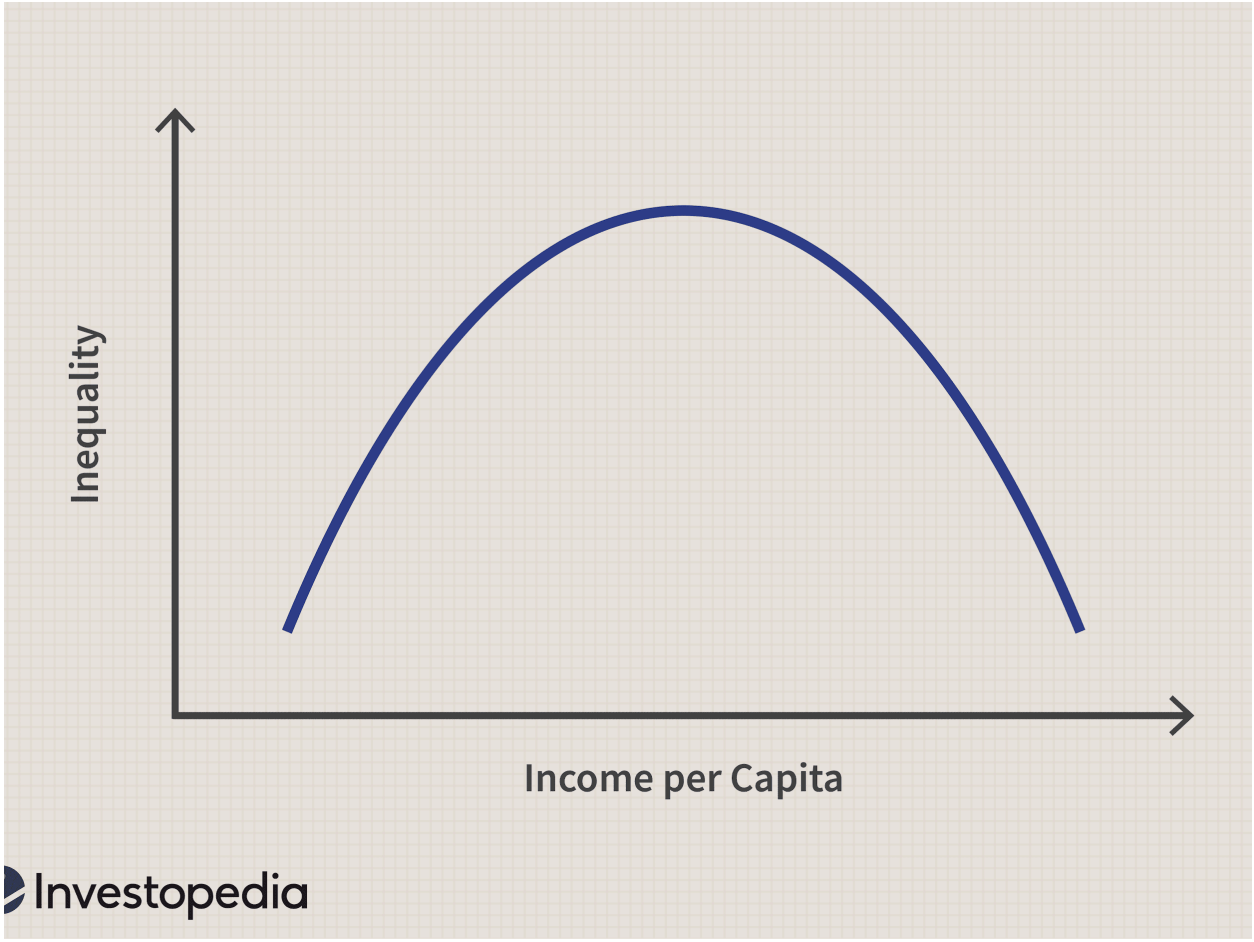
- Naxalism is not merely a law and order issue. The phenomenon of naxalism directly related to underdevelopment. Thus naxalism is not the problem rather it is the symptom of the problem.
- Issue of jal jameen jungle water land and forest
    - Migration
    - Land acquisition without proper or appropriate compensation and rehabilitation
    - Disruption of age old forest tribal relationship
    - Invasion of land ceiling laws
- Development deficit
    - Job deficit
    - Infrastructure deficit
- Governance deficit
- Social exclusion and alienation.
- Thus exploitation, underdeveloped agriculture, geographical isolation, lack of land reforms all contributed significantly towards the growth of naxal movement in India.
- In fact at the peak of this movement, this influence was seen to be spreading from Tirupati to Pashupati but at present the naxal influence is mainly prevalent across 30 district of seven States that is Jharkhand, Chhattisgarh, Odisha, Maharashtra, West Bengal, Andhra, Telangana and it is mainly concentrated in in Jharkhand and Chhattisgarh
- CPIM is the most potent left wing extremist organisation in the country listed under UAPA. At present naxals are trying to exploit new areas and various social

group and marginalised section like dalit and minorities through active association with their grievances against the state. CPIM has established closed strategic ties with many violent North East insurgent group like PLA of Manipur and NSCN-IM(of Nagaland) and it has frequently expressed it's solidarity with the terrorist group of J&K.

- CPIM has also established close links with Maoist group of Philippines and Turkey. It is also the member of CCOMPOSA (Coordination Committee of Maoist Party And Organisation of South Asia)--> it includes the Maoists group from India Bangladesh Nepal and Sri Lanka and its aim is to resist US imperialism and globalisation.
- And it is also targeted against the elites expansionist design of India in South Asia backed by US imperialism.
- Recently this organisation has retriated it's anti India stand and has reaffirm for its commitment to spread protracted people's war to capture States power through violent mean in South Asia.

Stand of state?

-



The term naxal derives its name from village naxalbari of district Darjeeling in West Bengal where this moment was originated in 1967 under the leadership of Charu Majumdar and Kanu Sanyal. Naxal are far left radical communist. Extreme communist derive their teaching from Mao Zedong and their believe is that
This doctrine naxal doctrine teachs to capture the state power true combination of

- Armed violence
- Mass mobilization
- Strategic alliances

India adopted democratic socialism.

Modern Right→ Ultra Right→ Extreme Right

Modern Left→ Ultra Left→ Extreme Left

Naxals are far-lefts, radical communists who derive their political ideology from the teachings of Mao Zedong, a Chinese revolutionary leader. Their belief is that the all existing social relations and state structures in an elitist, capitalist society are exploitative in nature and only a revolutionary change through violent means can end this exploitation. This doctrine teaches to capture the state power through combination of armed violence , mass mobilizations, and strategic alliances.
And they call this process has PPW (protracted people's war). Thus this ideology glorify violence. Political power grows out of the barrel of gun is the key slogan of naxals. Thus naxals are not seeking to secede from Indian Union to establish their sovereign rule of their own but their aim is to capture political power through arms struggle and to install the so called "People's Govt"
MNS in 2006 described Naxalism as the most significant of threat to the internal security of India.

Fight against naxalism?

- According to the state though from their ideology it appeared that naxals are fighting for the rights of the poor and want to establish peoples government but the facts are quite contradicting as according to the state social upliftment of the downtrodden is not their real aim rather it is the acquisition of political power
- Thus according to the state the only study local problems and issues and trying to use them as a fodder to foster their endgame which is clearly the seizure of power through violent means.
- According to the government it is the naxal who have vested interest in keeping the poverty alive as it enables them to expand their territory.
- And it is the naxals for not allowing the administration to do the developmental work. The social and economic issues of the people have taken a backseat and the battle of supremacy has emerged as the prime motto of naxals.
- In 2006 after PM's declaration of the naxal problem as the biggest threat to the national security, many new steps were taken by the government. And government decided to create a separate department in the home ministry with the name naxal management division and government appointed the expert committee and the committee in its report state that **lack of empowerment**

among the local community is the main reason for spread of naxalism committee is further stated that the state bureaucracy has failed miserably in delivering good governance in naxal affected areas. And government accepted that the fight against naxalism has to be long and persistent and government adopted **multipronged composite strategy** to counter this menace

a. Security measures- according to the state those who are hardcore ideologues who's only purpose is to overthrow the state have to be dealt strongly with the policy of bullet for bullet. As these people do not want development and they only want to use underdevelopment and governance deficit as the means to achieve their selfish goal
b. Development measures
c. Media and public perception management → naxals have a very powerful propaganda machinery which is active in all major cities as well as in national capital and they even have supporters in media. And they have frontal organisation and this NGO and activist wage a propagandist war against any government step that aims to check the naxal movement. Why they raise hue and cry? For Human Rights against police actions on naxals but these groups are conveniently silent when naxal use violent against people.
d. Cut down the financial support to naxal movement
e. Effective surrender and rehabilitation policy and ensuring proper safety and care for their family
f. According to government Doors for peace talk are always open

(Read Again the notes incomplete section)
Issue of Jal-Jameen-Jungle

Land acquisitions without appropriate compensation and rehabilitation.

Disruption of age old forest tribal relationship.

Evasion of land ceiling laws.

Developmental deficit

High poverty

Infrastructure deficit

Lack of education

Lack of employment opportunities

Governance Deficit:

Mismanagement and corruption in govt schemes

Lack of routine administration

Incompetence- illtrained and poorly motivated public personnels

Social exclusion and alienation:

Violation of their human rights

Abuse to the dignity of life has led to the discontent against the govt.

Disconnect with the mainstream

Thus, exploitation, underdeveloped agriculture, geographical isolation, lack of land reforms all contributed significantly towards the growth of naxal movement in India.

In fact, at the peak of this movement , this influence was seen to be spreading from Tirupati to Pashupati. But, at present the Naxal influence is prevalent mainly across 30 districts of 7 states that is, Jharkhand, chattisgarh, Orissa, Maharashtra, West Bengal, Andhra and telangana. And presently mainly concentrated in Jharkhand and chattisgarh.

CPIM is the most potent left wing extremist organization in the country listed in the UAPA. At present, Naxals are trying to exploit new areas and various social groups and marginalized sections like Dalits and minorities through active association with their grievances against the state. CPIM has established close strategic ties with many violent northeast insurgent groups like PLA of Manipur, and NSCN-IM of Nagaland and it has frequently expressed it's solidarity with the terrorist groups of J&K. CPIM has also established close links with the Maoist groups of Phillipines and Turkey. It is also the member of CCOMPOSA (Coordination Committee of Maoist parties and Organized Communities of south Asia) and it includes the Maoist groups from India, Bangladesh, Nepal and Sri Lanka. It's aim is to resist US imperialism and globalization. It is also targeted against the alleged expansionist designs of India in South Asia backed by US imperialism. Recently, this organization has recreated its anti-India stand and has reaffirmed its commitment to spread PPW to capture state power through violent means in South Asia.

Fight against Naxalism:

According to the state, though from their ideology it appears that Naxals are fighting for the rights of the poor and want to establish a people's government while the facts are quite contradictory as according to the state, social upliftment of the downtrodden is not their real aim rather it is the acquisition of political power.

Thus, according to the state, they only study local problems and issues and try to use them as fodder to foster their endgame which is clearly the seizure of power through violent means.

According to the govt, it is the Naxals who have vested interests in keeping poverty alive as it enables them to expand their territory. It is the Naxals who are not allowing the administration to do the developmental works. The social and economic issues of the people have taken a backseat and the battle of supremacy has emerged as the prime motto of the Naxals. In 2006, after PM'S declaration of the Naxal problem as the biggest threat to national security many new steps were taken by the Govt. One major step was the creation of a separate department in the Home Ministry with the name of 'Naxal Management Division ' and the govt appointed an expert committee

Internal security report by MHA

Operation greyhound?

Salwa judum?

Insurgency

- For the violence of the North East.

North East history

- There are more than a hundred tribal groups in the entire North Eastern region of India and they have a rich cultural heritage with a variety of customs and language. British gave special administrative status to these areas and British government decided not to disturb their socio-political structure and followed a deliberate policy of excluding the outsiders. (Under the policy of isolation) under this policy, outsiders were not allowed to acquire land in the tribal area. Thus during the British era non tribals were not penetrated to these areas to any significant extent. Thus there was a virtual absence of any political, cultural or economic contact of the tribals in the North East with the rest of the country.
- Also the freedom struggle the strong unitary for had very little impact on the tribal. After independence the government of India decided to give special attention to the tribal policy, realising the relative isolation of this region and the government decided to integrate the region with the rest of the mainland.
- After independence the government decided to make Assamese as the sole official language of the state which led to immediate and strong reaction from the hill tribal population as the tribal were afraid of losing their identity and being assimilated by the policy of assimilation. And the first and the foremost significant violent insurgency started in Naga area.

Issue of Nagaland

- After independence the government of India started the integration of Naga area with the state of Assam and India as a whole and the headliner naga leadership led by AZ Phizo opposed this decision and revolted in the banner of NNC and demanded separate sovereign state.

- And Phizo launched an armed rebellion against the government of India and the government of India decided to send an army to Nagaland to restore peace and order and thus by following the policy of separation and non negotiation the government formally opposed the secessionist demand for the independence of Naga areas.
- On the other hand the government realizes they need reconciliation and winning over the hearts of the naga people. As total physical suppression was neither feasible nor desirable and government started increasing the moderate Naga leadership to integrate with the rest of India in mind and spirit. And government started negotiation with the moderate nonviolent and non secessionist Naga leadership headed by doctor Imkongliba Ao and government refused to negotiate with hardliners and Phizo until they did not give up the demand of freedom
- Moderate Naga leadership agreed to negotiate with the government of India for separation of the separate state of Nagaland and after prolonged negotiation this happened and this step restored people's faith in the democratic values and values that are enshrined in our constitution.
- In 1975 government of India sign an agreement known as **Shillong Accord** with the various violent Naga groups under which the government announced that the government is ready to grant amnesty to all without any condition(punishment). If they are ready to accept the supremacy of the constitution of India and surrender their arms and renounce the demand for secession.
- Despite these steps violence still persists without any progress toward political settlement and instead the present situation may be better understood as a very complex set of relationships which exist between numbers of parties who are having different objectives, strategies and capability.
- In 1980→ Nationalist Socialist Council of Nagaland was formed by CS Isak and T. Muivah and S. S. Khaplang(Myanmar) and they were opposing the Shillong Accord signed by the Naga government with the government of India. (NSCN→ aims to form Nagalim[sovereign Nagaland])
- Naga→ Assam, Manipur, Arunachal, Myanmar
- Khaplang was pushing leader of Myanmar
- Isak and Muivah pushing Indian leader
- Opposition with a objective to establish sovereign state of Nagaland by unifying all the areas inhabited by the Naga in the North East and Myanmar but later misunderstanding surfaced out within the leaders of the outfit over the issue of commensation negotiation dialogue the government of India
- And NSCN split into two factions NSCN IM and K and in 1988 and this split triggered the violence and factional clashes between these two factions and though the objective of both were the same that is to achieve the objective of Nagalim that is to unify all the Naga habitat area into one.
- In 2001 NSCN-IM faction signed a ceasefire agreement with the government of India. And after the prolonged discussion Naga peace accord was signed in 2015 with the government of India with NSCN-IM.

Issues of Manipur (most violent state)

- There are more than 30 insurgent groups including the non violent one who are demanding independence from India.
- Apart from the fact that there are more violent group in the state then any where else and the rivalry between these groups leads to greater violence
- The three important Tribes of Manipur are
    a. Meitei → 60%
        - Majority are Hindu follower of Vaishnava tradition
        - Minority are Muslim and Christian
        - Live in the plain area of Manipur
        - Violent Insurgent Groups
            - Manipur People's Liberation Front
            - People's Liberation Army
            - United National Liberation Front
            - People's Revolutionary Party Of Kangleipak
            - They want a sovereign state
    b. Kuki → habited hill area
        - Violent insurgent group
            - Kuki National Organisation
            - United National Front
            - They are fighting for separate state for kuki with India
    c. Nagas → habited hill area
        - Naga insurgent group
            - NSCN IN
            - NSCN K
            - NSCN R
            - They want to annex the part of Manipur and merged with greater Nagaland
            - And these Naga
- State is having numerous conflict and violence between nagas and kuki and nagars and meites and meited and kuki
- Communal conflict between Hindu and Muslim meites
- State witnessed a lot of problems on the issue of implementation of ILP.

Issues with Arunachal Pradesh

- Tirap, Longding and Changlang are living in perpetual fear because of the presence of the cadre of NSCN IN and K factions
- As these three districts are part of their projected state of Nagalim. Apart from these Naga outfits, ULFA is having a strong presence in these regions and ULFA uses these three districts for infiltration into Myanmar where the base camp is located.
- ULFA uses these areas extensively for temporary transit camps while on the move and as well as to escape counter-insurgency in Assam.
- Another emerging concern is the presence of Maoist cadres that are Naxals and their presence is reported from Lohit and Lower Dibang Valley district. Another issue is the presence of 100000 strong communities of Chakmas and Hajong and they came to India from Chittagong hill tract from East Pakistan and they are Buddhist and Hindu and they entered into India that is in Arunachal during

1960s due to persecution. And in 2005 election commission of India issued guidelines to include chakmas and hajong in to the electoral roll of Indian election and in 2017 home ministry has allowed citizenship for Chakmas and Hajong communities and this has led to protest by All Arunachal Pradesh Student Union as according to AAPSU the presence of these refugees and the influx of other foreigners has resulted into the marginalisation of indigenous tribe.

- Porous borders leads to all this issue.

ASPA?

- An Indian Army soldier patrols near the line of control, the line that divides Kashmir between India and Pakistan, after a reported cease-fire violation, in Mendhar, Poonch district.
- The Armed Forces (Special Powers) Act was enacted in 1958 to bring under control what the government of India considered 'disturbed' areas. The Tripura government on Thursday decided to lift the controversial law which according to a Press Trust of India report "was in effect for the last 18 years to curb insurgency."
- The Act has often faced flak from human rights groups as it gave sweeping powers and immunity to the army in conflict-ridden areas.
- As of now, according to the home ministry, six more states come under the ambit of this law under various conditions. Here is a simple explainer to make sense of it all
- Assam, Nagaland, Manipur (except the Imphal municipal area), Arunachal Pradesh (only the Tirap, Changlang and Longding districts plus a 20-km belt bordering Assam), Meghalaya (confined to a 20-km belt bordering Assam) and Jammu and Kashmir.

Why is this required?

- The government (either the state or centre) considers those areas to be 'disturbed' "by reason of differences or disputes between members of different religious, racial, language or regional groups or castes or communities."

How does one officially declare a region to be 'disturbed'?

- Section (3) of the AFSPA Act empowers the governor of the state or Union territory to issue an official notification on The Gazette of India, following which the centre has the authority to send in armed forces for civilian aid. It is still unclear whether the governor has to prompt the centre to send in the army or whether the centre on its own sends in troops.
- Once declared 'disturbed', the region has to maintain status quo for a minimum of three months, according to The Disturbed Areas (Special Courts) Act, 1976.

Is the act uniform?

- No. Originally, it came into being as an ordinance in 1958 and within months was repealed and passed as an Act. But, this was meant only for Assam and Manipur, where there was insurgency by Naga militants. But after the northeastern states were reorganized in 1971, the creation of new states (some of them union territories originally) like Manipur, Tripura, Meghalaya, Mizoram and Arunachal Pradesh paved the way for the AFSPA Act to be amended, so that it could be

applied to each of them. They may contain different sections as applicable to the situation in each state.

- This moment was finally ended when the central government signed the agreement with the leaders of AASU
- Thus the Assam Accord on 15 August 1985 under which it was decided that those who entered the state in between 1st January 1966 to march 1971 will be allowed to remain in Assam but will be disenfranchised for 10 years. And those who will enter after 1971 will face expulsion
- NRC was conducted under judicial interview

There are several organisations that advocate the independence of Assam from India and the most prominent is ULFA and it has two main goals one that is independence of Assam and second that is establishment of socialist governance.

Issue of bodoland

- Bodo is the largest plain tribe of Assam and they started an armed struggle for the sovereign state in 1980. And they started violence against non Bodo
- In 2003 government signed the **Bodoland Territorial Council** accord with Bodo leaders to end their violent movement and under this accord government created **Bodoland Territorial Area District**
- 4 contiguous district of Assam→ 2, 25, 24, 26
- However within bodoland territorial area district the non Bodo were against the creation of BTAD as they were demanding the cancellation of villages having less than 50% of the population of bodo from BTAD. However various fractions of **National Democratic Front Of Bodoland** was seeking to obtain a sovereign Bodoland and in January 2020 the government had signed a peace pact with the four factions of NDFB for the permanent solution of Bodo issues.

Issue of Karbi Anglong district

- One of the most backward districts of Assam.
- The dominant tribe of this district is karbi
- And the violent outfit is Karbi People's Liberation Tiger and they are demanding separate state for Karbi
- Adama asking the separate state
- KPLP using violence against the Rengamas
- And the violent outfit of Rengamas is
    - Rangama Naga Hills Protection Force
    - And they are demanding more autonomy from rengamas
    - And to protect rangama from the violent attack of karbi

Issue of Kamtapur

- Kamtapur Liberation Organisation and its objective is to carb out sovereign state of Kamtapur in India

- And their proposed state comprises of four district of Assam
- It was formed to address the problem of Rajbounshi people

Issues of Meghalaya

- Violent insurgent group of Meghalaya GNLA - garo national liberation army and its objectives to establish separate/sovereign garoland for the garo people and this organisation is under UAPA
- ANVC- Achik National Volunteer Council aims to carve out a separate state for Achik within garoland.
- HNLC- Hynniewtrep National Liberation Council representative of khasi jayanti people's and it seems to free Meghalaya from the domination of Garos

Issue of Tripura

- Violence is reduced drastically in Tripura
- AFSA has been lifted from Tripura
- All this led to due to Manik Sarkar government
- To violent outfits of Tripura having secessionist agenda NLFT- national liberation front of Tripura
- ATTF -

Lack of visionary leaders around the tribals

Cyber threats

- Cyberspace is a complex environment consisting of the interaction between people and software and services supported by the world wide distribution of information and communication technology and network
- Today cyber space is used as a common pool by the citizens, businesses, government and military in a manner that makes it difficult to draw the clear boundary among these different groups.
- Cyber space is expected to be more complex in the foreseeable future with many fold increase in the devices and the network connected to it
- Cyberspace can be broadly classified into two groups
    a. Cyber crime-it is illegal activity done using digital devices and networks against individuals and corporate that to for financial and material gains. In involves any of the following that is digital devices as the target through virus and malware and Dos attack and denial of service
        - To store illegal data is a crime
        - Using digital devices to commit crime and fraud
    b. Crime war- it involves the action by a nation state to damage another Nation's critical infrastructure through viruses or dos attack. It is considered as fifth domain of warfare
        - It is a information warfare
        - If there any cyber attack on it then US will defend 5th domain by resorting to the purposanate attack by other 4 domain and the similar stand is kept up by Russia and China
        - The use of STUXNET virus that a malware against Iran's nuclear warfare was indeed a case of nation state against cyber war

        - New term electronic terrorism
- Cyber security policy→ EJ Snowden an american computer professional and formal employee of CIA disclosed to several major media outlets thousands of classified documents uncovering the existence of numerous global surveillance program run by the US government and this release of classified documents has been described as the most significant leak in US history and the US department of justice has charged snowden of espionage. The document reveals that the surveillance was also directed against India.
- Through his revelations the government of India came to know that our cyberspace is unprotected.
- The national cyber security policy 2013 build a secure and resilient cyberspace and under this government has listed the Critical Computer Infrastructure which needs special protection against cyber attack.
- **CCI**→ it is information communication technology devices on which the core functionality of critical infrastructures dependent. Critical infrastructure are those facilities, functions and systems whose incapacity and destruction can cause a debilitating impact on national security, governance, economy and social well being of the nation. And it includes sectors like Banking and Finance, space establishment and nuclear power plants and sensitive defence and government organisations, air transportation.

Naxalism

Naxalism....1
Naxalism: Historical Evolution and Phases - Phase 1: Origins (1967-1972)....1
Topic: Naxalbari Uprising, Ideological Foundations, Key Leaders & Demands, Case Study....1
Phase 2: First Split and Decline (1972-1980)....2
Topic: Internal Conflicts, Government Response, Changes in Strategy....2
Phase 3: Resurgence (1980-2004)....3
Topic: New Geographical Spread, Changed Tactics, Formation of Major Groups, Case Study: PWG and MCC Operations....3
Post-Merger Period (2004-present)....4
Topic: Formation of CPI(Maoist), Modern Challenges, Current Status, Data: Recent Statistics on Affected Areas....4
Constitutional and Administrative Framework: Fifth Schedule Provisions....5
Topic: Key Features, Implementation Status, Gaps and Challenges, Case Study: PESA Act Implementation....5
Tribal Rights and Development....6
Topic: Forest Rights, Land Acquisition Issues, Development Displacement, Example: Specific Tribal Displacement Cases....6
Socio-economic Factors....7
Topic: Poverty and Inequality, Land Issues, Education and Healthcare, Data: HDI Indicators in Affected Areas....7
Security Dimensions....8
Topic: Current Challenges, Affected Regions, Strategic Importance, Case Study: Recent Security Operations....8
Development Issues....9
Topic: Infrastructure Gaps, Industrial Development Impacts, Resource Allocation, Example: Development Projects in Affected Areas....9
Government Response and Strategy: Security Measures....11
Topic: Operations and Campaigns, Coordination Mechanisms, Modernization Efforts, Data: Security Force Deployment....11
Government Response and Strategy: Development Initiatives....12
Topic: Special Schemes, Infrastructure Development, Skill Development, Case Study: Success Stories....12
Government Response and Strategy: Political and Administrative Measures....13
Topic: Surrender Policies, Rehabilitation Packages, Governance Reforms, Example: Successful Rehabilitation Case....13
Committees....14
Expert Group on "Development Challenges in Extremist-Affected Areas" (2008)....14
2. Committee on Prevention of Extremism (2008)....14
3. Expert Group on Left Wing Extremism (2011)....14
4. Administrative Reforms Commission (ARC) - 2nd Report on "Public Order" (2007)....14
5. Planning Commission Task Force on Naxalism (2008)....15
6. Supreme Court and High Court Observations....15
7. Reddy Committee Report (2006)....15

Naxalism: Historical Evolution and Phases - Phase 1: Origins (1967-1972)

Topic: Naxalbari Uprising, Ideological Foundations, Key Leaders & Demands, Case Study

A. Naxalbari Uprising (1967): The Genesis of Naxalism

- **Peasant revolt against feudal landowners** in Naxalbari, West Bengal.
    - Sparked by failure of CPI-M led United Front to implement land reforms.
- **Inspired by the communist movement**, aimed at land redistribution.
    - A response to India retaining the colonial land tenancy system.

B. Ideological Foundations: A Blend of Marxism, Leninism, and Maoism

- **Rejection of parliamentary democracy**, advocating for **violent revolution**.
    - Saw the Chinese Communist Party's path as the model for India.
- **Emphasis on "annihilation of class enemies"** to achieve revolution.
    - Targeted landlords and those perceived as oppressive forces.
- **Influence of Charu Mazumdar's Historic Eight Documents (1965).**
    - Outlined the ideological and strategic framework for the Naxalite movement.

C. Key Leaders and Demands

- **Charu Mazumdar:** Chief ideologue and strategist of the movement.
    - Advocated for guerrilla warfare and annihilation of class enemies.
- **Kanu Sanyal:** Key organizer among Santhal tribals in Darjeeling.
    - Instrumental in sparking the Naxalbari uprising.
- **Core Demands:** Land redistribution, ending exploitation of peasants and tribals, and establishment of a communist state.
    - Reflected deep-seated grievances against socio-economic injustices.

D. Case Study: The Original Naxalbari Movement

- **Rapid Spread:** From West Bengal to Bihar, Andhra Pradesh, and other states.
    - Exploited existing unrest among marginalized communities.
- **Violent Tactics:** Armed struggle against landowners, police, and state authorities.
    - Used limited weaponry, including bows and arrows initially.
- **Government Response:** Initially perceived as a law and order problem.
    - Resulted in violent crackdowns and suppression of the movement by 1972.
- **Legacy:** Established the blueprint for future Naxalite insurgencies in India.
    - Demonstrated the potential for exploiting rural grievances and the state's vulnerability.

E. Concluding Remarks

- The Naxalbari uprising marked the birth of Naxalism in India, driven by ideological convictions and socio-economic disparities.
- The movement's early phase was characterized by a fervent belief in violent revolution and the leadership of figures like Charu Mazumdar and Kanu Sanyal.
- Despite its eventual suppression, the Naxalbari movement laid the foundation for the protracted Naxalite struggle that continues to challenge India's security and development.

Phase 2: First Split and Decline (1972-1980)

Topic: Internal Conflicts, Government Response, Changes in Strategy

A. Internal Conflicts and Fragmentation (1972-1980)

- **Death of Charu Mazumdar (1972):** Created a leadership vacuum.
    - Triggered intense debates over ideology, strategy, and leadership within the movement.
- **Emergence of Factions:** Movement splintered into numerous smaller groups.
    - Notable factions: CPI-ML (Liberation), CPI-ML (Party Unity), MCC, and others.
- **Ideological Disputes:** Disagreements on the path to revolution intensified.
    - Debates on annihilation strategy, mass movements, and role of the urban proletariat.

B. Government Response: A Multi-Pronged Approach

- **Intensified Crackdown:** Aggressive police and paramilitary operations against Naxalites.
    - Efforts to dismantle Naxalite networks and apprehend key leaders.
- **Strategic Shift:** From solely law-and-order approach to a combination of security and development measures.
    - Recognized the socio-economic roots of the Naxalite insurgency.
- **Implementation of Land Reforms:** Aimed at addressing agrarian grievances.
    - Limited success due to corruption and lack of political will.

C. Changes in Naxalite Strategy: Adaptation and Survival

- **Decline in Annihilation Strategy:** Recognized its limitations and counterproductive nature.
    - Shift towards a more nuanced approach, focusing on building mass support.
- **Emphasis on Mass Mobilization:** Organizing peasants and tribals around socio-economic issues.
    - Formation of frontal organizations to work on issues like land rights, wages, and forest produce.
- **Guerrilla Warfare Tactics:** Continued reliance on small-scale attacks and ambushes.
    - Exploitation of difficult terrain and support bases in remote areas.

D. Concluding Remarks

- The period 1972-1980 witnessed the fragmentation of the Naxalite movement, triggered by internal conflicts and the government's intensified crackdown.
- The movement's decline was marked by a shift away from the annihilation strategy towards a focus on mass mobilization and building support bases.
- The government's response transitioned towards a multi-pronged approach, incorporating security measures with attempts at addressing socio-economic grievances.

Phase 3: Resurgence (1980-2004)

Topic: New Geographical Spread, Changed Tactics, Formation of Major Groups, Case Study: PWG and MCC Operations

A. New Geographical Spread: Expanding the "Red Corridor"

- Naxalism expanded beyond its initial strongholds in West Bengal and Andhra Pradesh.
    - Spread to new areas like Bihar, Jharkhand, Chhattisgarh, and Maharashtra.
- Exploited **underdevelopment and socio-economic marginalization** in these regions.
    - Targeted areas rich in natural resources, attracting recruits among disaffected communities.
- The "Red Corridor" concept emerged, envisioning a contiguous Maoist-controlled territory.
    - Strategic aim of connecting Naxalite-affected areas from Nepal to Andhra Pradesh.

B. Changed Tactics: Adapting to New Realities

- **Shift from individual annihilation to targeting economic and infrastructure assets.**
    - Attacks on railways, mines, power stations, and industrial complexes.

- **Increased focus on recruitment and training of armed cadres.**
    - Formation of the People's Guerrilla Army (PGA), a dedicated military wing.
- **Sophistication in weaponry and tactics**, moving beyond basic arms.
    - Acquisition of modern firearms, explosives, and communication equipment.

C. Formation of Major Groups: Consolidation and Unification

- **People's War Group (PWG) in Andhra Pradesh emerged as a dominant force.**
    - Known for its organizational strength, military capabilities, and mass base.
- **Maoist Communist Center (MCC) in Bihar and Jharkhand gained prominence.**
    - Focused on building rural support, engaging in armed actions against state forces.
- **Efforts towards greater unity among Naxalite factions**, leading to mergers.
    - The PWG and MCC merged in 2004 to form the CPI-Maoist.

D. Case Study: PWG and MCC Operations

1. PWG in Andhra Pradesh

- **Dominated the Naxalite landscape** in the state during this period.
    - Successfully established control in several districts, challenging state authority.
- **Employed a combination of mass mobilization and armed struggle.** (, Table 1)
    - Organized peasant movements, provided basic services, and conducted targeted killings.
- **Faced strong resistance from the Andhra Pradesh government.**
    - Formation of specialized police units like the Greyhounds to counter the PWG.

2. MCC in Bihar and Jharkhand

- **Gained a foothold in the underdeveloped and tribal-dominated regions.**
    - Exploited grievances against state neglect, land alienation, and poverty.
- **Focused on building a mass base among rural communities.**
    - Organized village-level committees, provided dispute resolution, and welfare services.
- **Engaged in armed actions against police**, landlords, and perceived class enemies.
    - Targeted attacks, ambushes, and extortion to assert control and disrupt governance.

E. Concluding Remarks

- The period 1980-2004 witnessed a resurgence of Naxalism, marked by geographical expansion, tactical evolution, and the consolidation of major groups.
- The PWG and MCC emerged as dominant forces, demonstrating the movement's adaptability and resilience.
- Their operations, particularly in Andhra Pradesh, Bihar, and Jharkhand, highlighted the challenges posed to state authority and the complexities of addressing the Naxalite issue.

"The Resurgence of Naxalism: How Great a Threat to India?". It details Naxalite violence in Andhra Pradesh from 1985 to 1990 and is used to illustrate the growing violence employed by the PWG under the leadership of Kondapalli Seetharamaiah.
Demonstrates a pattern of increasing attacks on jotedars (landlords), police, and police informants during this period

Post-Merger Period (2004-present)

Topic: Formation of CPI(Maoist), Modern Challenges, Current Status, Data: Recent Statistics on Affected Areas

A. Formation of CPI(Maoist): A Unified Threat

- The **merger of the PWG and MCC in 2004** created the CPI(Maoist).
    - Became the **largest and most potent Naxalite group in India**.

- **Aims to overthrow the Indian state** through protracted people's war.
    - Employs a combination of **armed struggle and mass mobilization**.
- **Strategic goal of establishing a "Compact Revolutionary Zone" (CRZ)**.
    - Envisions a **contiguous Maoist-controlled territory** spanning eastern and central India.

B. Modern Challenges: Evolving Threat Landscape

- **Increased sophistication in tactics and weaponry**.
    - Use of **improvised explosive devices (IEDs), landmines, and advanced firearms**.
- **Formation of a dedicated military wing, the People's Liberation Guerrilla Army (PLGA)**.
    - **Estimated to have thousands of armed cadres** organized into platoons and companies.
- **Expansion into new geographical areas**, including states like Odisha and Maharashtra.
    - **Exploitation of underdevelopment, tribal grievances, and lack of governance**.
- **Growing nexus with criminal networks and other insurgent groups**.
    - Allegations of **links with Pakistani intelligence agencies and the LTTE**.
- **Challenges in countering the CPI(Maoist)'s ideology and propaganda**.
    - Effective use of **social media and local networks** to spread their message.

C. Current Status: A Persistent Challenge

- **CPI(Maoist) remains active in over 200 districts across 10 states**. (, Figure 1,)
    - Continues to pose a **significant threat to internal security and development**.
- **Government response has been multi-pronged**, but with limited success.
    - Combines **security operations, development initiatives, and surrender schemes**.
- **Naxalism continues to cause violence and displacement**.
    - **Thousands of civilians, security personnel, and Naxalites have been killed** since 2004.
- **Debate on the root causes and appropriate countermeasures persists**.
    - Balancing **security and development approaches** remains a challenge.

D. Data: Recent Statistics on Affected Areas

- **192 districts in 16 states were affected by Maoist activity in early 2008**.
    - Covers a significant portion of India's landmass and population.
- **An average of 417 civilians killed annually in Naxalite violence since 2010**.
    - Highlights the **human cost of the conflict**.
- **Maoist-related violent incidents have decreased by 26.7% from 2013 to 2018**.
    - Indicates some **success in government countermeasures**.
- **But the CPI(Maoist) remains a resilient and adaptable adversary**.
    - Continued need for a **holistic and sustained approach** to address the issue.

Constitutional and Administrative Framework: Fifth Schedule Provisions

Topic: Key Features, Implementation Status, Gaps and Challenges, Case Study: PESA Act Implementation

A. Key Features of Fifth Schedule Provisions

- **Empowers the President to declare "Scheduled Areas"** within states.
    - Primarily **inhabitated by tribal populations** requiring special protection.

- **Establishes Tribal Advisory Councils (TACs)** to advise on tribal affairs.
    - Composed of **tribal representatives** and nominated members.
- **Grants special powers to Governors** to regulate land, resources, and customary laws.
    - Can **adapt laws and policies** to suit local tribal needs.
- **Aims to safeguard tribal rights**, promote development, and maintain peace.
    - **Addresses historical injustices and vulnerabilities** faced by tribal communities.

B. Implementation Status: A Mixed Record

- **Fifth Schedule provisions have been implemented** in various states.
    - But the **effectiveness varies** due to factors like political will and capacity.
- **TACs have been established**, but their **functioning and influence are often limited**.
    - Lack of **adequate resources, representation, and enforcement mechanisms**.
- **Governors' powers have been exercised** to enact special regulations.
    - But **implementation challenges** and bureaucratic hurdles persist.

C. Gaps and Challenges: Obstacles to Effectiveness

- **Lack of awareness and understanding** of Fifth Schedule provisions.
    - Among both **tribal communities and government officials**.
- **Political interference and lack of commitment** to tribal welfare.
    - Prioritization of **economic interests over tribal rights** in some cases.
- **Inadequate funding and capacity** for implementation.
    - **Shortage of trained personnel** and resources to execute programs.
- **Weak enforcement mechanisms** and accountability.
    - Limited **monitoring and evaluation** of the impact of Fifth Schedule provisions.

D. Case Study: PESA Act Implementation: Challenges Persist

- **The Panchayat (Extension to Scheduled Areas) Act, 1996 (PESA)**.
    - Aimed to **empower Gram Sabhas** (village assemblies) in Scheduled Areas.
- **Provides for greater control over local resources**, development, and governance.
    - **Recognizes traditional governance systems** and customary laws.
- **Implementation has been uneven and faced challenges**.
    - Lack of **political will, awareness, and capacity at the local level**.
- **Conflicts between traditional and modern governance structures**.
    - **Domination by non-tribal elites** in some Gram Sabhas.

E. Concluding Remarks

- The Fifth Schedule provisions offer a **constitutional framework for tribal welfare and autonomy**.
- But their **implementation has been hampered by various gaps and challenges**.
- Addressing these issues requires a **multi-pronged approach**, including:
    - **Raising awareness, strengthening institutions, ensuring political commitment, and providing adequate resources**.
- The **PESA Act serves as a case study**, highlighting the complexities and opportunities in **implementing tribal self-governance**.

Tribal Rights and Development

Topic: Forest Rights, Land Acquisition Issues, Development Displacement, Example: Specific Tribal Displacement Cases

A. Forest Rights: Contested Terrain

- **Tribals have historically depended on forests** for livelihood and cultural practices.
    - Provides sustenance, resources, and spiritual connection.
- **Forest laws often restrict tribal access and control over forest resources.**
    - Leading to conflicts and displacement.
- **Forest Rights Act (FRA), 2006, recognizes tribal rights over forest land and resources.**
    - Grants individual and community rights, including ownership, use, and management.
- **Implementation of FRA remains uneven and faces challenges.**
    - Lack of awareness, bureaucratic hurdles, and resistance from vested interests.

B. Land Acquisition Issues: Displacement and Dispossession

- **Land acquisition for development projects often displaces tribal communities.**
    - Mining, dams, industries, and infrastructure projects.
- **Inadequate compensation and rehabilitation measures** exacerbate the problem.
    - Loss of land, livelihood, and cultural heritage.
- **Land acquisition laws and policies need to prioritize tribal rights and consent.**
    - Ensure fair compensation, meaningful consultation, and sustainable development.

C. Development Displacement: A Complex Challenge

- **Development projects can bring benefits, but also risks for tribal communities.**
    - Economic opportunities, infrastructure, and social services.
- **Displacement can lead to impoverishment, social disruption, and loss of identity.**
    - Severing ties to land, community, and traditional practices.
- **Development needs to be inclusive and sensitive to tribal rights and aspirations.**
    - Prioritize local participation, cultural preservation, and equitable benefit sharing.

D. Example: Specific Tribal Displacement Cases

- **Naxal-affected areas witness significant tribal displacement due to mining and infrastructure projects.**
    - Loss of ancestral lands and forests, leading to social and economic marginalization.
- **Adivasis in Chhattisgarh have been displaced by mining operations and Salwa Judum campaigns.**
    - Forced displacement, human rights violations, and militarization of the region.
- **Displacement of tribal communities for dams and irrigation projects in various states.**
    - Submergence of villages, loss of agricultural land, and displacement to unfamiliar environments.

E. Concluding Remarks

- Tribal rights and development are intertwined and require a balanced approach.
- Addressing forest rights, land acquisition issues, and development displacement is crucial for tribal welfare and peace in Naxal-affected areas.
- Policy measures should focus on:
    - Recognizing and protecting tribal rights, ensuring fair compensation and rehabilitation, promoting inclusive development, and fostering cultural preservation.
- Specific cases of tribal displacement highlight the need for greater sensitivity, accountability, and justice in development processes.

Socio-economic Factors

Topic: Poverty and Inequality, Land Issues, Education and Healthcare, Data: HDI Indicators in Affected Areas

A. Poverty and Inequality: Fueling Discontent

- **Naxal-affected areas are characterized by high levels of poverty and income inequality.**
    - Creating a fertile ground for **grievances and social unrest**.
- **Lack of access to basic necessities** like food, water, and sanitation.
    - Contributing to **poor health, low productivity, and vulnerability to exploitation**.
- **Disparities in income and wealth** between tribal communities and others.
    - **Marginalization and exclusion** from economic opportunities.

B. Land Issues: Core Grievance

- **Land is central to tribal livelihoods, identity, and culture.**
    - Source of sustenance, security, and social cohesion.
- **Historical dispossession and exploitation of tribal land by non-tribals.**
    - Forced displacement, land alienation, and denial of customary rights.
- **Land reforms and policies have often failed to address tribal concerns.**
    - **Inadequate implementation, loopholes, and corruption**, benefitting vested interests.

C. Education and Healthcare: Deprivation and Neglect

- **Naxal-affected areas have low literacy rates and poor access to quality education.**
    - **Lack of schools, teachers, infrastructure, and culturally relevant curriculum**.
- **Healthcare facilities are inadequate and inaccessible**, leading to high morbidity and mortality.
    - **Shortage of doctors, medicines, and infrastructure**, compounded by geographical remoteness.
- **Poor health and education outcomes** perpetuate the cycle of poverty and vulnerability.
    - Limiting opportunities for **social and economic advancement**.

D. Data: HDI Indicators in Affected Areas: Reflecting Deprivation

- **HDI indicators (Human Development Index)** in Naxal-affected areas are significantly lower than national averages.
    - Reflecting **poor human development outcomes** across various dimensions.
- **Low life expectancy, literacy rates, and per capita income** are common features.
    - Indicating **systemic deprivation** and underdevelopment.
- **HDI data provides empirical evidence** of the socio-economic challenges in these regions.
    - Highlighting the **urgent need for targeted interventions and investments**.

E. Concluding Remarks

- Socio-economic factors play a crucial role in the emergence and persistence of Naxalism.
- Poverty, inequality, land issues, and lack of basic services create a breeding ground for discontent and rebellion.
- **Addressing these issues is essential for tackling the root causes of Naxalism** and promoting sustainable peace and development.
- **HDI data underscores the need for a multi-sectoral approach**, focusing on poverty alleviation, land reforms, education, healthcare, and inclusive growth.

Security Dimensions

Topic: Current Challenges, Affected Regions, Strategic Importance, Case Study: Recent Security Operations

A. Current Challenges: A Complex Security Landscape

- **Growing sophistication and lethality of Naxal attacks:** Targeting security forces, infrastructure, and economic assets.
    - Use of **IEDs, landmines, and sophisticated weaponry,** increasing casualties and disrupting development.
- **Expansion of Naxal influence: "Red Corridor"** spreading across multiple states, challenging state authority.
    - **192 districts across 16 states** affected by Naxal violence and mobilization in 2008.
- **Nexus with other insurgent groups:** Collaboration with Northeast insurgent groups and international Maoist organizations.
    - **Shared ideology, training, and logistical support**, posing a greater threat to internal security.
- **Exploitation of local grievances:** Using **socio-economic disparities** to recruit and gain support.
    - **Poverty, inequality, land alienation, and lack of development**, fueling Naxal ideology and mobilization.

B. Affected Regions: The "Red Corridor" and Beyond

- **Central and Eastern India:** Primarily affecting states like **Chhattisgarh, Jharkhand, Odisha, Bihar, and Maharashtra**.
    - **Dense forests, hilly terrain, and poor infrastructure**, providing a haven for Naxal operations.
- **Expansion into new areas:** Gradual spread towards **southern and western states** like Andhra Pradesh, Telangana, and Karnataka.
    - **Exploiting vulnerabilities and seeking new recruits and resources.**
- **Potential spread to Northeast India:** Concerns about Naxal infiltration into states with pre-existing insurgencies.
    - **Similar socio-economic conditions and porous borders** with Nepal and Bangladesh.

C. Strategic Importance: Implications for National Security

- **Threat to internal stability:** Undermining governance, disrupting development, and challenging state legitimacy.
    - **Creating a climate of fear and instability**, impeding economic growth and social progress.
- **Economic implications:** Targeting infrastructure, mining operations, and industries, impacting national development.
    - **Disrupting supply chains, hindering investment, and causing economic losses**.
- **Challenge to democratic institutions:** Seeking to overthrow the Indian state through armed struggle.
    - **Undermining democratic processes, rule of law, and human rights**.

D. Case Study: Recent Security Operations

- **Operation Green Hunt (2009-2010):** A multi-state operation involving central and state security forces to combat Naxal violence.
    - **Mixed results:** Some successes in containing Naxal activities, but also facing criticism for human rights violations.
- **State-specific operations:** Andhra Pradesh's "Greyhounds" unit, known for its effectiveness in counter-insurgency operations.

    - **Specialized training, intelligence gathering, and rapid response tactics**, proving successful in containing Naxalism in the state.
- **Challenges in security operations:** Difficult terrain, lack of intelligence, and the need to balance security measures with human rights concerns.
    - **Naxal use of human shields, landmines, and guerrilla tactics**, posing significant challenges for security forces.

E. Concluding Remarks

- **Naxalism poses a significant security challenge to India**, requiring a multi-pronged approach combining security and developmental measures.
- **Addressing current challenges, understanding affected regions, and recognizing the strategic importance** of countering Naxalism is crucial for national security.
- **Security operations need to be conducted with sensitivity and accountability**, ensuring human rights are protected while effectively countering violence.
- **Recent security operations highlight both successes and challenges**, informing future strategies and emphasizing the need for a comprehensive approach.

Development Issues

Topic: Infrastructure Gaps, Industrial Development Impacts, Resource Allocation, Example: Development Projects in Affected Areas

A. Infrastructure Gaps: Hindering Development and Accessibility

- **Naxal-affected areas suffer from significant infrastructure deficits**, including roads, electricity, communication, and healthcare facilities.
    - **Limiting access to basic services**, markets, and opportunities for economic and social development.
- **Poor road connectivity** hampers transportation, trade, and government service delivery.
    - **Isolating communities**, increasing vulnerability, and hindering economic growth.
- **Lack of electricity and communication networks** limits access to information, education, and healthcare services.
    - **Perpetuating underdevelopment and hindering efforts to improve living standards**.

B. Industrial Development Impacts: A Double-Edged Sword

- **Industrial development in mineral-rich areas often leads to displacement of tribal communities and environmental degradation**.
    - **Creating resentment and fueling Naxal recruitment**, as tribals perceive exploitation and loss of livelihoods.
- **Lack of inclusive development:** Benefits of industrial growth often fail to reach local communities.
    - **Widening the gap between the rich and poor**, exacerbating inequalities and grievances.
- **Need for sustainable and inclusive industrial development:** Balancing economic growth with social and environmental considerations.
    - **Ensuring equitable sharing of benefits and minimizing negative impacts on tribal communities**.

C. Resource Allocation: Addressing Disparities and Prioritizing Development

- **Inadequate resource allocation to Naxal-affected areas**: Perpetuating underdevelopment and hindering efforts to address root causes.

    - **Need for increased investment in infrastructure, education, healthcare, and livelihood programs**.
- **Prioritizing development in conflict zones:** A crucial aspect of a comprehensive counter-insurgency strategy.
    - **Addressing socio-economic grievances** to reduce support for Naxal ideology and promote peace.
- **Ensuring transparency and accountability in resource allocation:** Building trust and fostering community participation in development processes.
    - **Empowering local communities** to manage resources and prioritize their development needs.

D. Example: Development Projects in Affected Areas

- **Pradhan Mantri Gram Sadak Yojana (PMGSY):** A rural road connectivity program implemented in Naxal-affected areas.
    - **Aiming to improve access to markets, services, and economic opportunities**.
- **National Rural Employment Guarantee Programme (NREGP):** Providing guaranteed wage employment in rural areas, including Naxal-affected districts.
    - **Creating employment opportunities, generating income, and reducing poverty**.
- **Challenges in project implementation:** Security concerns, difficult terrain, lack of skilled labor, and corruption.
    - **Need for effective monitoring, community participation, and grievance redressal mechanisms**.

E. Concluding Remarks

- **Development issues are intertwined with the Naxal problem**, requiring a holistic and integrated approach.
- **Addressing infrastructure gaps, mitigating industrial development impacts, and prioritizing resource allocation** are crucial for sustainable peace and development.
- **Development projects need to be designed and implemented with sensitivity**, ensuring community participation and equitable distribution of benefits.
- **Effective governance, transparency, and accountability** are essential for development initiatives to succeed in Naxal-affected areas.

Government Response and Strategy: Security Measures

Topic: Operations and Campaigns, Coordination Mechanisms, Modernization Efforts, Data: Security Force Deployment

A. Operations and Campaigns: Combating Naxal Violence

- **Security forces conduct operations to disrupt Naxal activities** and reclaim control of affected areas.
    - **Example:** Operation Green Hunt (2009-2010), a major offensive against Naxal strongholds.
- **Challenges**: Difficult terrain, guerrilla tactics, civilian casualties, and human rights concerns.
    - **Controversial use of vigilante groups**, like Salwa Judum, raising ethical and legal questions.
- **Need for intelligence-based operations**, minimizing collateral damage, and adhering to human rights principles.

B. Coordination Mechanisms: Fostering Inter-Agency Cooperation

- **Unified Command structure:** Established to coordinate efforts between central and state security forces.

    - **Facilitates intelligence sharing, joint operations, and resource allocation**.
- **Inter-state cooperation**: Crucial for addressing cross-border movement of Naxal cadres.
    - **Joint task forces and intelligence sharing mechanisms** established to enhance coordination.
- **Challenges**: Bureaucratic hurdles, lack of trust between agencies, and political interference.
    - **Need for streamlined decision-making, clear lines of responsibility, and effective communication**.

C. Modernization Efforts: Enhancing Capabilities of Security Forces

- **Modernization of state police forces**: Upgrading weapons, communication systems, and training facilities.
    - **Funding provided by the central government** through schemes like the Security Related Expenditure (SRE) Scheme.
- **Special Forces**: Creation of specialized units trained in counter-insurgency and jungle warfare.
    - **Examples**: Greyhounds in Andhra Pradesh, Special Task Force (STF) in Chhattisgarh.
- **Technological advancements**: Use of Unmanned Aerial Vehicles (UAVs) for surveillance and intelligence gathering.

D. Data: Security Force Deployment

- **Central Armed Police Forces (CAPF) battalions deployed to support state police forces**.
    - **As of 2008, 36 CAPF battalions were deployed in Naxal-affected areas**.
- **Indian Reserve (IR) battalions**: Raised to strengthen security in affected states.
    - **Providing additional security and employment opportunities for local youth**.

E. Concluding Remarks

- **Government's security response to Naxalism focuses on a multi-pronged strategy**, combining operations, coordination, and modernization.
- **Challenges remain in addressing operational complexities**, ensuring effective coordination, and balancing security measures with human rights considerations.
- **Data on security force deployment highlights** the significant resources allocated to combating Naxalism.
    - Security Related Expenditure (SRE) scheme is recurring and continuous in nature. In last 05 years Rs. 1685.65 crore have been released to the Left Wing Extremism (LWE) affected states.

Government Response and Strategy: Development Initiatives

Topic: Special Schemes, Infrastructure Development, Skill Development, Case Study: Success Stories

A. Special Schemes: Targeting Naxal-Affected Areas

- **Government implements schemes to address socio-economic grievances** and promote development in Naxal-affected regions.
    - **Focus on poverty reduction**, employment generation, education, healthcare, and infrastructure development.
- **Security Related Expenditure (SRE) Scheme**: Provides funds to states for modernization of police forces and infrastructure development in LWE affected areas.
    - **Rs. 2299 Crore released to states since 2014-15**.
- **Special Infrastructure Scheme (SIS)**: Funds projects to upgrade Special Forces, intelligence agencies, and fortify police stations.
    - **Approved projects worth Rs. 991.04 crore during 2017-21**.

- **Backwards Districts Initiative (BDI) and Backwards Region Grant Fund (BRGF)**: Focus on development of backward districts, including many Naxal-affected areas.

B. Infrastructure Development: Connecting Remote Areas

- **Recognizing the link between underdevelopment and Naxalism**, the government prioritizes infrastructure projects in affected regions.
    - **Road construction**, electrification, communication networks, and irrigation facilities are crucial for development and connectivity.
- **Pradhan Mantri Gram Sadak Yojana (PMGSY)**: Aims to connect all villages with all-weather roads, facilitating access to markets and services.
- **Challenges**: Security concerns, difficult terrain, and funding constraints can hinder implementation.

C. Skill Development: Empowering Youth for Employment

- **Skill development programs target youth in Naxal-affected areas**, providing them with marketable skills and employment opportunities.
    - **Reduces vulnerability to Naxal recruitment** and promotes economic independence.
- **Vocational training centers**, entrepreneurship development programs, and job placement assistance are provided.
- **Challenges:** Lack of awareness, limited access to training centers, and mismatch between skills and industry demands.

D. Case Study: Success Stories

- **Andhra Pradesh**: The state's Greyhounds police unit and focused development initiatives have significantly weakened Naxal presence.
    - **Effective surrender and rehabilitation policy** encouraged Naxal cadres to renounce violence and reintegrate into society.
- **Lessons Learned**: Combining security operations with focused development initiatives can yield positive results.
    - **Importance of good governance**, addressing local grievances, and winning the trust of communities.

E. Concluding Remarks

- **Development initiatives are a crucial aspect of the government's counter-Naxal strategy**, aiming to address root causes and promote sustainable peace.
- **Special schemes**, infrastructure development, and skill development programs target the socio-economic needs of affected communities.
- **Success stories, like Andhra Pradesh**, demonstrate the effectiveness of a holistic approach that combines security measures with development efforts.
- **Challenges remain in implementation**, particularly in ensuring effective resource allocation, community participation, and good governance.

Government Response and Strategy: Political and Administrative Measures

Topic: Surrender Policies, Rehabilitation Packages, Governance Reforms, Example: Successful Rehabilitation Case

A. Surrender Policies: Encouraging Disengagement

- **Government offers surrender and rehabilitation policies to encourage Naxal cadres to lay down arms**.
    - **Aim**: To wean away disillusioned cadres and weaken Naxal organizations.
- **Policies include financial assistance**, vocational training, and support for reintegration into mainstream society.
    - **Andhra Pradesh offers houses worth Rs. 1 lakh and employment**.
- **Challenges**: Ensuring the genuineness of surrenders, preventing re-joining, and addressing the needs of surrendered cadres.

B. Rehabilitation Packages: Supporting Reintegration

- **Comprehensive rehabilitation packages are essential for successful reintegration of surrendered Naxal cadres**.
    - **Packages include housing, education, healthcare, and livelihood support**.
- **Focus on addressing the specific needs of women and children** affected by Naxalism.
    - **Counseling**, skill development, and educational opportunities.
- **Challenges**: Lack of adequate funding, bureaucratic hurdles, and social stigma can hinder effective rehabilitation.

C. Governance Reforms: Addressing Root Causes

- **Government recognizes the importance of good governance in tackling Naxalism**.
    - **Addressing corruption, improving service delivery, and ensuring equitable distribution of resources**.
- **Empowering local communities through Panchayati Raj institutions**, enabling them to participate in decision-making.
- **Challenges**: Political interference, lack of capacity in local administrations, and resistance from vested interests.

D. Example: Successful Rehabilitation Case

- **Andhra Pradesh's surrender and rehabilitation policy has been relatively successful**.
    - **Combined with effective police action, it significantly reduced Naxal violence**.
- **Key factors**: Strong political will, adequate funding, and a focus on socio-economic development.

E. Concluding Remarks

- **Political and administrative measures are essential complements to security operations in counter-Naxal strategy**.
- **Surrender policies, rehabilitation packages, and governance reforms aim to address the root causes of the problem** and provide alternatives to violence.
- **Successful cases, like Andhra Pradesh**, demonstrate the importance of a holistic and integrated approach.
- **Sustained efforts are required to overcome challenges** and ensure long-term peace and development in affected regions.

Committees

Expert Group on "Development Challenges in Extremist-Affected Areas" (2008)

- **Chairperson**: D. Bandopadhyay
- **Suggestions**:
    - Enhance **land reforms** to address socio-economic grievances.
    - Strengthen **tribal rights**, especially over forest lands (implementation of FRA 2006).

- Promote **inclusive development** in affected areas (healthcare, education, infrastructure).
- Increase **local governance** through Panchayati Raj Institutions (PRIs).

---

2. Committee on Prevention of Extremism (2008)

- **Chairperson**: K.S. Subramanian
- **Suggestions**:
  - Reform **policing and justice systems** to address human rights violations.
  - Promote **trust-building measures** between state agencies and locals.
  - Develop **confidence-building mechanisms**, including impartial grievance redressal systems.

---

3. Expert Group on Left Wing Extremism (2011)

- **Chairperson**: Ajit Doval
- **Suggestions**:
  - Strengthen **intelligence sharing** among states and central agencies.
  - Build a **multi-agency task force** for coordinated anti-Naxal operations.
  - Deploy a mix of **development programs and military interventions** in Naxal-prone areas.
  - Improve communication infrastructure for better monitoring.

---

4. Administrative Reforms Commission (ARC) - 2nd Report on "Public Order" (2007)

- **Suggestions**:
  - Strengthen **civil administration** and reduce reliance on armed forces for internal security.
  - Focus on the **root causes**, including economic disparity and land issues.
  - Ensure **transparent governance** in tribal regions.
  - Improve the functioning of **Special Police Officers (SPOs)** and training of security forces.

---

5. Planning Commission Task Force on Naxalism (2008)

- **Suggestions**:
  - Accelerate the **implementation of welfare schemes** like MGNREGA in Naxal-affected areas.
  - Create **livelihood opportunities** to reduce the dependency of locals on Naxal cadres.
  - Monitor the **proper utilization of funds** allocated to development programs.

---

6. Supreme Court and High Court Observations

- **Recent Judgments**:
  - Emphasize on upholding **human rights** during counterinsurgency operations.
  - Critique the **state-sponsored Salwa Judum movement**, citing excessive violence.

---

7. Reddy Committee Report (2006)

- **Suggestions**:
  - Prioritize **dialogue over violence** for resolving the conflict.
  - Address the **grievances of displaced populations** due to industrial and mining activities.

Role of external state and non-state actors in creating challenges to internal security..... 1
Definition of Internal Security..... 1
Key Actors..... 1
State Actors..... 1
Key Actors..... 2
Non-State Actors..... 2
Threats to Internal Security (Broad Categories)..... 3
Terrorism (Cross-Border & Domestic)..... 3
Insurgency (Naxalism, North-East)..... 3
Organized Crime (Drug trafficking, human trafficking, money laundering)..... 4
Communal Violence..... 4
Radicalization..... 5
Cyber Security Threats..... 5
Regionalism and Separatism..... 5
Left-Wing Extremism:..... 6
Piracy:..... 6
Challenges related to border management:..... 6
Terrorism:..... 7
Types of Terrorism:..... 7
Causes of Terrorism:..... 7
Funding Sources of Terrorist Groups..... 7
Modus Operandi:..... 7
Counter-Terrorism Strategies:..... 8
Neighboring Countries (China, Pakistan, Sri Lanka)..... 8
China:..... 8
Pakistan:..... 9
Sri Lanka:..... 9
Strategic Partnerships & Economic Corridors..... 10
Military & Economic Influence..... 10
Historical Context:..... 10
Current Strategic Relationship:..... 10
Areas of Cooperation:..... 10
Areas of Conflict:..... 11
Economic Implications:..... 11
Security Implications:..... 11
Indian Response Strategy:..... 11
Case Studies:..... 11
Over-Ground Workers (OGWs)..... 11
Religious & Ethnic Groups..... 12
1. Historical Context:..... 12
2. Current Strategic Relationship:..... 12
3. Areas of Cooperation:..... 12
4. Areas of Conflict:..... 12
5. Economic Implications:..... 12

6. Security Implications: 12
7. Indian Response Strategy: 12
8. Case Studies: 13
Role of Non-State Actors in Creating Challenges to Internal Security: Maritime Pirates 13
1. Historical Context: 13
2. Current Strategic Relationship: 13
3. Areas of Cooperation: 13
4. Areas of Conflict: 13
5. Economic Implications: 13
6. Security Implications: 13
7. Indian Response Strategy: 13
8. Case Studies: 13
Cross-Cutting Themes 14
Radicalization: 14
Economic Security: 14
Border Management: 14
Regional Stability: 14
Immediate Neighbors 14
1. Pakistan: 14
2. China: 14
3. Sri Lanka: 15
Extended Neighbors 15
Indian Ocean Region: 15
Central Asia: 15
Southeast Asia: 15
China-Pakistan Economic Corridor (CPEC) 15
1. Strategic Implications: 15
2. Economic Impact: 15
3. Security Challenges: 16
4. Indian Response: 16
5. Future Scenarios: 16
Radicalization 16
1. Root Causes: 16
2. Vulnerable Groups: 16
3. Prevention Strategies: 16
4. Deradicalization Programs: 17
5. International Best Practices: 17
Maritime Security 17
Recent Cases (Post-2020) 17
Historical Cases 18

Role of external state and non-state actors in creating challenges to internal security

Definition of Internal Security

- **Internal security** safeguards a nation's core values, institutions, and well-being from threats within its boundaries.
    - It is distinct from **external security**, which deals with threats from foreign countries.
- **Responsibility for internal security** lies with the state police, supported by central police forces.
    - **Armed forces** are responsible for maintaining external security.
- Internal security challenges require **unconventional warfare skills**, while external threats involve conventional warfare.
- **Threats to internal security** include Naxalism, communalism, and terrorism.
    - **External threats** include challenges from hostile neighbors and maritime security issues.
- **Terrorism in India** often involves external state and non-state actors, including Pakistan and ISI.
    - External actors provide support for terrorism through finance, training, and ideology.
- **India's internal security architecture** needs changes to effectively counter-terrorism.
    - Recommendations include enhancing intelligence capabilities and strengthening the police force.
- **International cooperation** is essential to combat terrorism effectively.
    - However, a lack of global consensus on defining terrorism poses a challenge.
- **Examples of internal security challenges** include the J&K situation, North Eastern issues, and Naxalism.
    - Strategies to address these challenges include deploying specialized forces and implementing development programs.
- **Cybersecurity** is a growing concern for both internal and external security.
    - This requires strengthening national cyber infrastructure and international collaboration.
- **Disasters**, both natural and man-made, also pose a significant challenge to internal security.
    - The NDRF plays a crucial role in disaster response.

Concept Explanation: Internal security encompasses measures taken to protect a nation's people, institutions, and way of life from threats originating within its own borders.

Key Actors

State Actors

- **Government** plays a crucial role in maintaining internal security.
    - This involves policy formulation, resource allocation, and coordination among various agencies.
- **Security forces**, including police and paramilitary forces, enforce law and order.
    - Central Armed Police Forces (CAPF) guard borders and protect sensitive establishments.
    - Specialized forces like NSG combat terrorism and handle hijacking situations.
- **Intelligence agencies** are responsible for gathering information to counter threats.
    - Intelligence Bureau (IB) handles internal security intelligence.
    - Research and Analysis Wing (RAW) gathers intelligence from external threats.
    - There are concerns about a lack of accountability and coordination among intelligence agencies.
- **Ministry of Home Affairs** is the primary agency responsible for internal security.
    - It oversees the functioning of police forces, paramilitary forces, and intelligence agencies.

- **Armed Forces** are called upon to support internal security when necessary.
    - They play a direct role in counter-insurgency operations in J&K and Northeastern states.
    - Their indirect role includes providing support for disaster relief and other emergencies.
- **Cabinet Committee on Security (CCS)** is the apex body for executive action on national security matters.
    - It approves the raising of new battalions for security forces like ITBP.
- **National Security Council (NSC)** advises the government on national security policy.
    - It comprises various groups, including the National Security Advisory Board and the Strategic Policy Group.
    - There is a debate on giving NSC more powers and making the NSA accountable to Parliament.
- **Department of Military Affairs (DMA)** is headed by the Chief of Defence Staff (CDS).
    - CDS provides impartial advice to the political leadership on defense matters.
- **Other agencies** play a role in specific aspects of internal security, like narcotics control.
    - Narcotics Control Bureau (NCB) tackles drug trafficking.

Concept Explanation: State actors in internal security are government entities with a mandated role in protecting national security and maintaining order. This includes various departments, agencies, and security forces.

The K.C. Pant Task Force in the late 1990s had recommended the creation of an NSA with the rank of a Cabinet Minister.

More powers to NSC: If the NSC is to be made more useful, the government's allocation of business rules should be amended to give more powers to the NSC and its subordinate organisations, such as the Strategic Policy Group.

Key Actors

Non-State Actors

- **Terrorist groups** aim to destabilize the country through violence and fear.
    - They operate with support from external states like Pakistan.
    - Examples include Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM).
- **Insurgent groups** challenge state authority through armed rebellion.
    - They operate in areas like J&K and the Northeast.
    - Examples include United Liberation Front of Assam (ULFA) and National Democratic Front of Bodoland (NDFB).
- **Organized crime syndicates** engage in illegal activities for profit.
    - They often have cross-border connections and operate in areas like drug trafficking and human trafficking.
- **Radicalized groups** promote extremist ideologies and incite violence.
    - Lone wolf attacks by self-radicalized individuals pose a serious challenge.
    - The internet and social media are used for radicalization and recruitment.
- **NGOs** can sometimes pose a challenge to internal security.
    - They are accused of misusing funds and inciting discontent against development projects.
- **Over Ground Workers (OGWs)** provide logistical and other support to terrorist groups.

Concept Explanation: Non-state actors are entities that operate outside of government control and can pose threats to internal security through various means, including violence, crime, and subversion.

Threats to Internal Security (Broad Categories)

Terrorism (Cross-Border & Domestic)

- **Terrorism** involves the use of violence to create fear and achieve political goals.
    - **Cross-border terrorism** originates from external state and non-state actors.
    - **Domestic terrorism** arises from internal factors and may have linkages to external actors.
- **Pakistan** is a major source of cross-border terrorism in India.
    - **ISI** provides support to terrorist groups like LeT and JeM.
    - The 26/11 Mumbai attacks highlight the threat of cross-border terrorism.
- **Terrorism in J&K** is a major internal security challenge.
    - It is fueled by Pakistan's support for separatist groups and cross-border infiltration.
    - The government has deployed specialized forces like the NSG to counter terrorism in J&K.
- **Hinterland terrorism** by groups like Indian Mujahideen (IM) and Students Islamic Movement of India (SIMI) is another concern.
    - These groups may receive indirect support from Pakistan.
- **Counter-terrorism strategies** involve intelligence gathering, security measures, and legal frameworks.
    - The government has strengthened anti-terrorism laws like UAPA and NIA Act.
- **International cooperation** is crucial to combat terrorism effectively.
    - However, a lack of global consensus on defining terrorism poses a challenge.

Concept Explanation: Terrorism can be categorized as cross-border when it originates from external actors or domestic when it arises from internal factors. Both pose significant challenges to internal security and require comprehensive strategies to combat them effectively.

Insurgency (Naxalism, North-East)

- **Insurgency** involves armed rebellion against state authority.
    - **Naxalism** is a left-wing extremist insurgency operating in central India.
        - It is considered a significant internal security threat.
    - **Insurgency in the Northeast** is fueled by ethnic and separatist demands.
- **Naxal affected areas** have seen violence and disruption of development activities.
    - The government has implemented a multi-pronged strategy involving security, development, and rehabilitation.
- **Insurgent groups in the Northeast** operate across porous borders with countries like Myanmar.
    - Assam Rifles plays a key role in counter-insurgency operations in the Northeast.
- **Challenges in countering insurgency** include:
    - Difficult terrain and porous borders
    - Weak local intelligence gathering
    - Ideological support in urban areas (Urban Naxalism)
    - Involvement of external actors in providing support
- **Government measures to counter Naxalism**:
    - Security Related Expenditure (SRE) Scheme
    - Special Infrastructure Scheme (SIS)
    - SAMADHAAN - a comprehensive strategy for counter-insurgency
    - Integrated Action Plan (IAP) to address development deficits
    - Road Requirement Plan for extremist affected areas
    - Roshani Scheme for skill development
- **Reforms suggested for security forces**:
    - Increasing professionalism and attracting talent
    - Creating a coordinating center for effective intelligence sharing
    - Addressing issues related to encounters and training of frontline officers

Concept Explanation: Insurgency poses a significant challenge to internal security by undermining state authority and disrupting peace and development. Addressing insurgency requires a comprehensive approach that combines security measures with development initiatives and addresses the root causes of the conflict.

The **Roshani Scheme** is a placement-linked skill development program implemented by the Ministry of Rural Development. It aims to provide skills training and employment opportunities to youth in extremist-affected areas. This scheme helps counter the influence of extremist groups by offering alternative pathways to economic empowerment and social integration.

Organized Crime (Drug trafficking, human trafficking, money laundering)

- **Organized crime** involves continuing serious criminal activities for profit.
    - **Transnational crime** is flourishing, particularly threatening fragile states.
- **Drug abuse and trafficking** are serious organized crimes with transnational linkages.
    - India is a transit point for drugs from the Golden Triangle and Golden Crescent.
- **Human trafficking and smuggling** are significant concerns for internal security.
- **Money laundering** involves concealing the origins of illegally obtained money.
    - Criminal networks launder assets abroad before investing them.
- **Countermeasures** involve:
    - Dismantling criminal networks and raising barriers to their operations.
    - Financial investigations and seizure of assets.
- **International cooperation** is crucial to fight transnational crime effectively.
    - This involves sharing intelligence, coordinating law enforcement efforts, and strengthening legal frameworks.
- **Challenges** include:
    - Porous borders and weak law enforcement capacity in some regions.
    - Corruption and involvement of powerful individuals in organized crime.

Concept Explanation: Organized crime poses a significant threat to internal security by undermining the rule of law, fueling violence, and generating illicit profits. Addressing organized crime requires a multi-pronged approach involving law enforcement, intelligence gathering, international cooperation, and addressing the root causes such as poverty and inequality.

Communal Violence

- **Communal violence** involves violence between religious or ethnic groups.
    - It can be instigated by external actors or internal factors.
    - It poses a serious threat to social harmony and national integration.
- **Proxy wars** can fuel communal tensions in India.
    - External powers may support groups to exploit religious fault lines.
- **Pakistan's ISI** has been accused of supporting communal violence in India.
    - This is aimed at destabilizing India and undermining its secular fabric.
- **Social media** can be used to spread rumors and incite violence.
    - This highlights the need for effective monitoring and regulation of online platforms.
- **Measures to counter communal violence**:
    - Promoting interfaith dialogue and harmony.
    - Strengthening law enforcement and ensuring swift justice.
    - Addressing the root causes of communal tensions.

Concept Explanation: Communal violence is a complex issue with multiple causes, including historical grievances, political opportunism, and socioeconomic disparities. It can be exacerbated by external actors seeking to destabilize a country. Effective countermeasures require a holistic approach that combines security measures with social and economic initiatives.

Radicalization

- **Radicalization** is the process of adopting extreme political, social, or religious views.
    - It can lead to violence and terrorism.

- **Lone wolf attacks** are a growing concern globally.
    - These are attacks by self-radicalized individuals without direct support from terrorist organizations.
- **The internet** plays a significant role in radicalization.
    - Online platforms provide access to extremist propaganda and facilitate recruitment.
- **Factors contributing to radicalization**:
    - Social alienation and marginalization
    - Perceived injustices and grievances
    - Ideological indoctrination
- **Counter-radicalization strategies**:
    - Promoting critical thinking and media literacy
    - Addressing grievances and providing alternative narratives
    - Engaging with communities and religious leaders

Concept Explanation: Radicalization is a gradual process that can transform individuals into extremists willing to resort to violence. It is a complex phenomenon driven by a combination of individual, social, and ideological factors. Countering radicalization requires a multi-faceted approach that addresses both the push and pull factors that contribute to it.

Cyber Security Threats

- **Cyberattacks** can disrupt critical infrastructure and steal sensitive information.
    - **Espionage** by state actors is a significant cyber threat.
    - **Cybercrime** is a growing threat, often motivated by financial gain.
- **Vulnerability** is increasing due to the growing use of ICT platforms.
    - **Awareness of cyber security risks** is lagging behind the growth of internet use.
- **International cooperation** is essential to combat cyber threats effectively.
    - This includes agreements on standards of conduct and information sharing.
- **Public-private partnerships** are crucial to enhance cyber security.
    - The private sector possesses valuable expertise and resources.
- **National Cyber Security Strategy (NCSS)** provides a framework for cyber security in India.
    - The **National Cyber Security Council** coordinates preventive measures.
- **Capacity building** is crucial to develop a skilled cybersecurity workforce.

Concept Explanation: Cyber security threats are a growing concern, posing significant risks to national security, economic stability, and social well-being. These threats can originate from state actors, non-state actors, or criminal organizations. Addressing these threats requires a comprehensive approach involving technological measures, legal frameworks, international cooperation, and public awareness campaigns.

Regionalism and Separatism

- **Regionalism** is the expression of a common regional identity and the pursuit of regional interests.
- **Separatism** is a movement advocating for secession from a larger political entity.
- **Insurgency** is an organized rebellion against a constituted authority.
- **External state actors** can exploit regional and separatist sentiments to destabilize India.
    - Providing support to insurgent groups or engaging in propaganda.
- **Pakistan's ISI** has been accused of supporting separatist movements in India.
    - Particularly in Jammu and Kashmir and the Northeast.
- **Internal factors** contributing to regionalism and separatism:
    - Economic disparities, social inequalities, and political marginalization.
    - Perceived discrimination and lack of representation.
- **Measures to address regionalism and separatism**:
    - Promoting inclusive development and equitable distribution of resources.

    - Addressing grievances and ensuring political representation.
    - Strengthening law enforcement and counter-insurgency capabilities.

Concept Explanation: Regionalism and separatism pose serious challenges to national unity and territorial integrity. They can be exacerbated by external actors seeking to weaken a country. Addressing these challenges requires a multifaceted approach involving political dialogue, socioeconomic development, and security measures.

Left-Wing Extremism:

- **Naxalism** is a significant internal security threat in India.
    - Former PM Manmohan Singh termed it the most critical internal security threat.
- Naxalites employ violence to destabilize the Indian state.
    - They use communist guerrilla tactics and radical communist ideology.
- **External states support Naxalites.**
    - Providing aid, funding, training, and weapons, potentially escalating conflict.
- **Challenges in countering Naxalism:**
    - Weak local intelligence gathering and dissemination.
    - Rise of urban Naxalism and ideological supporters.
    - External support from neighboring countries.
- **Government initiatives to counter Naxalism:**
    - Road Requirement Plan for LWE affected areas in 8 states (Ministry of Road Transport and Highways).
    - Integrated Action Plan (IAP) with INR 6000 crore funding per year.
    - Security, public perception management, development, and rehabilitation.

Piracy:

- **Maritime security threats include piracy**, IUU fishing, and climate change.
- **India's coastal security is challenged by porous borders**.
    - Difficult terrain, inadequate patrolling, and terrorist infiltration.
- **Indian agencies responsible for maritime security**:
    - State Marine Police for inner layer patrolling.
    - Indian Coast Guard for maritime zone patrols.
    - Indian Navy for support within and beyond maritime zones.

Challenges related to border management:

- **India faces border management challenges due to difficult terrain**.
    - Deserts, mountains, rivers, and dense forests pose difficulties.
- **Porous borders allow for illegal activities**.
    - Smuggling, terrorist infiltration, and cross-border crime.
- **India-Nepal border challenges**:
    - Increasing extremism and ISI activities.
    - Fear of Maoist insurgency spreading.
- **ITBP plays a crucial role in border management**.
    - Provides security at sensitive installations.
    - The government has approved seven new ITBP battalions.
- **Need for a unified security agency:**
    - With advanced training and resources to guard borders.
    - Pooling resources of CAPF and Assam Rifles for enhanced security.
- **China's actions impact global consensus on terrorism**.
    - Blocking India's attempts to designate individuals as terrorists at the UN.
- **China's stance reflects a lack of global consensus on terrorism**.
    - Differing definitions and political considerations dilute efforts.
    - Bilateral interests and regional dynamics also play a role.

- **India needs to engage bilaterally and multilaterally**.
    - Pursuing global consensus while addressing specific concerns with China.

Terrorism:

Types of Terrorism:

- **Cross-Border Terrorism:** Terrorist acts originating from outside a country's borders.
    - *Pakistan's involvement in terrorism in Jammu and Kashmir* .
- **Homegrown Terrorism:** Terrorist acts perpetrated by individuals or groups within a country.
    - *Indian Mujahideen or SIMI indirectly supported by ISI* .
- **Ideological Terrorism:** Terrorism driven by specific beliefs or ideologies.
    - *Extremist Jihadist ideology propagating suicide terrorism in Kashmir* .

Causes of Terrorism:

- **Socio-Economic Grievances:** Poverty, unemployment, lack of opportunities, and inequality can fuel terrorism.
    - *Development work and its actual implementation on the ground* is imperative .
- **Political Grievances:** Oppression, discrimination, lack of political representation, and human rights abuses can lead to terrorism.
    - *Government must give priority to defeating political subversions by terrorists* .
- **Religious Grievances:** Extremist interpretations of religion, perceived threats to religious beliefs, and religious conflicts can motivate terrorist acts.
    - *SIMI aims at "Jihad" (religious war) for the cause of Islam* .
    - *Open expressions of support for jihadist activity among young people* .

Funding Sources of Terrorist Groups

- Terrorist groups rely on **diverse funding sources**.
    - Kidnapping for ransom, drug trafficking, and extortion.
- **External states may provide financial support to terrorist groups**.
    - Aiming to destabilize rival nations or advance geopolitical goals.
- **Terror financing through legitimate channels**:
    - Misuse and misappropriation of funds by NGOs.
- **Hawala networks and informal financial systems** are used for funding:
    - Exploiting gaps in financial regulations for illicit transfers.
- **Counterfeit currency is a major source of terror funding in India**.
    - Strengthening the Unlawful Activities (Prevention) Act, 1967.
- **India combats terror financing through legislative measures**.
    - Terror Funding and Fake Currency (TFFC) Cell in NIA
- **International cooperation is crucial to disrupt terror financing**.
    - India's membership in FATF, APG, EAG.

Modus Operandi:

- **Recruitment:** Terrorist groups use **propaganda and indoctrination**.
    - Exploiting social media and online platforms.
- **Training:** Terrorists receive **physical and ideological training**.
    - Provided in camps, safe havens, or online modules.
- **Use of Technology:** Terrorist groups leverage technology for **communication, recruitment, and attacks**.
    - Encrypted messaging apps, drones, and social media.
- **Over-ground Workers: Non-combatant supporters** provide logistical, financial, and intelligence support.
    - Individuals integrated into society.
- **Lone wolf attacks are increasing in prevalence**.
    - Presenting challenges for intelligence and security agencies.

Counter-Terrorism Strategies:

- **Legal Framework (UAPA):** India uses **UAPA to combat terrorism** by criminalizing unlawful activities.
    - Amended in 2019 to strengthen counter-terrorism measures.
- **Intelligence Gathering:** Effective **intelligence is crucial to disrupt terror plots**.
    - National Intelligence Coordinator recommended for better coordination.
- **Security Forces Operations: Specialized forces conduct counter-terrorism operations**.
    - National Security Guard (NSG) is India's premier counter-terrorist force.
- **Community Engagement: Engaging communities** helps counter radicalization and builds trust.
    - CVE strategies target disaffected sectors of society.
- **Financial Crackdown:** Disrupting **terror financing** is key to weakening terrorist groups.
    - India is a member of FATF and other international bodies.

Neighboring Countries (China, Pakistan, Sri Lanka)

China:

- **Historical Context: India and China share a complex history** marked by border disputes and the 1962 war.
    - The Line of Actual Control (LAC) remains a point of contention.
- **Current Strategic Relationship: Competition and cooperation coexist** in the India-China relationship.
    - Both countries are major economic and military powers in Asia.
- **Areas of Cooperation: Economic ties are growing**, with trade and investment increasing steadily.
    - India and China engage in multilateral forums like BRICS and the SCO.
- **Areas of Conflict: The border dispute remains unresolved**, leading to tensions and military buildup.
    - China's support for Pakistan and its growing influence in South Asia concern India.
- **Economic Implications:** China's economic rise presents both **opportunities and challenges for India**.
    - Competition for resources and markets, but also potential for collaboration.
- **Security Implications: China's military modernization** and assertiveness raise security concerns for India.
    - Increased military presence in the Indian Ocean and support for Pakistan.
- **Indian Response Strategy:** India is **modernizing its military**, strengthening alliances, and engaging diplomatically.
    - Focus on enhancing border infrastructure and developing partnerships with other countries.
- **Future Scenarios: The relationship is likely to remain competitive**, with potential for both conflict and cooperation.
    - The trajectory will depend on how both countries manage their strategic interests and the border dispute.
- **Case Studies:** Doklam standoff (2017), Galwan Valley clash (2020).
    - Incidents highlight the potential for escalation and the need for effective crisis management.

Pakistan:

- **Historical Context: India and Pakistan have a history of conflict**, including three major wars since independence.
    - The Kashmir issue remains the primary source of tension.
- **Current Strategic Relationship: Relations are marked by mistrust and hostility**, with limited dialogue.

    - Terrorism emanating from Pakistan is a major challenge for India.
- **Areas of Cooperation: Limited cooperation** on issues like trade, water sharing, and people-to-people contacts.
    - Sporadic attempts at dialogue have not yielded sustained progress.
- **Areas of Conflict: Terrorism, Kashmir, and border disputes** are the main sources of conflict.
    - Pakistan's support for anti-India terrorist groups is a major concern.
- **Economic Implications: Conflict and tensions hinder economic cooperation** and regional integration.
    - Trade potential remains largely untapped due to political obstacles.
- **Security Implications: Terrorism emanating from Pakistan** poses a significant threat to India's internal security.
    - Cross-border infiltration and attacks continue to occur.
- **Indian Response Strategy: Combating terrorism**, strengthening border security, and pursuing diplomacy.
    - India has taken a firm stance against Pakistan-sponsored terrorism.
- **Future Scenarios: Relations are likely to remain strained**, with the potential for escalation depending on events.
    - The resolution of the Kashmir issue and progress on counter-terrorism are crucial for improvement.
- **Case Studies:** Mumbai attacks (2008), Uri attack (2016), Pulwama attack (2019).
    - Highlight the ongoing threat of terrorism and the challenges in bilateral relations.

Sri Lanka:

- **Historical Context: India and Sri Lanka have a long history of cultural and economic ties**.
    - However, the Sri Lankan civil war and India's involvement had a complex impact.
- **Current Strategic Relationship: India and Sri Lanka are seeking to enhance cooperation** in various fields.
    - Shared security concerns in the Indian Ocean region.
- **Areas of Cooperation: Economic ties**, defense cooperation, development assistance, and people-to-people contacts.
    - India has provided significant support to Sri Lanka.
- **Areas of Conflict: Concerns over China's growing influence** in Sri Lanka and the treatment of Tamil minorities.
    - India seeks to balance its interests with Sri Lanka's sovereignty.
- **Economic Implications: Increased economic cooperation** and potential for regional integration.
    - India is a major investor and trading partner for Sri Lanka.
- **Security Implications: Shared security concerns** in the Indian Ocean region, including maritime security and terrorism.
    - Cooperation on intelligence sharing and capacity building.
- **Indian Response Strategy: Diplomacy, development assistance, and security cooperation**.
    - India seeks to maintain its influence and address its concerns through engagement.
- **Future Scenarios: The relationship is likely to evolve**, with India seeking to counter China's influence.
    - Sri Lanka's domestic political situation and its foreign policy choices will be key factors.
- **Case Studies:** India's involvement in the Sri Lankan civil war (1987-1990), the Hambantota port project.
    - Illustrate the complexities and challenges in the relationship.

Strategic Partnerships & Economic Corridors

Quadrilateral Security Dialogue (Quad), comprising **Australia, the United States, Japan, and India**, as a strategic partnership relevant to the Indo-Pacific region. This partnership, while not a formal military alliance, aims to address shared security concerns, including:

- **Maritime security:** Countering China's growing influence in the Indian Ocean Region.
- **Terrorism:** Collaboration on intelligence sharing and capacity building.
- **Cybersecurity:** Cooperation on norms and capacity building.

While the Quad presents a cooperative framework, potential conflicts could arise from:

- **Diverging interests** of member states within the Indo-Pacific.
- **Perceptions of the Quad as an anti-China alliance**, leading to regional tensions.

Economic corridors, such as the **China-Pakistan Economic Corridor (CPEC)**, can also have security implications for India. While such corridors aim to boost regional connectivity and trade, they also raise concerns:

- **Passage of CPEC through Pakistan-occupied Kashmir**, challenging India's territorial claims.
- **Potential use of economic corridors for military purposes**, impacting regional security dynamics.

India's response strategy includes:

- **Active participation in the Quad**, strengthening strategic partnerships.
- **Developing alternative connectivity projects**, countering China's Belt and Road Initiative.
- **Military modernization and enhanced border security**, addressing potential threats.

Case Studies:

- **The Quad's joint naval exercises and information sharing initiatives.**
- **India's concerns over the CPEC and its impact on regional stability.**

Military & Economic Influence

Historical Context:

- **Post-colonial era saw interference** from major powers during the Cold War.
- **Neighboring countries' involvement** in India's internal affairs, especially Pakistan.
    - Support for insurgency in Kashmir and Punjab.

Current Strategic Relationship:

- **China's rising economic and military power** significantly impacts regional dynamics.
    - Competition and cooperation coexist in India-China relations.
- **Pakistan remains a major source of tension**, with continued support for terrorist groups.
    - Limited cooperation and deep mistrust characterize the relationship.

Areas of Cooperation:

- **Economic ties with China are growing**, despite strategic competition.
    - Bilateral trade reached over $100 billion in 2021.
- **Limited cooperation with Pakistan** on issues like trade and water sharing.
    - Sporadic dialogues and confidence-building measures.

Areas of Conflict:

- **Border disputes with China**, unresolved for decades, lead to tensions.
    - Military buildup and incidents along the LAC.
- **Pakistan's support for terrorism** is a major challenge for India's internal security.
    - Cross-border infiltration, attacks, and proxy warfare.

Economic Implications:

- **China's economic influence** presents both opportunities and challenges for India.
    - Competition for markets and resources, but also potential for collaboration.
- **Conflict with Pakistan hinders economic growth** and regional integration.
    - Trade potential remains largely untapped due to political obstacles.

Security Implications:
- **China's military modernization** and assertiveness raise security concerns for India.
    - Increased military presence in the Indian Ocean and support for Pakistan.
- **Pakistan-sponsored terrorism** poses a significant threat to India's internal security.
    - Continued attacks and radicalization efforts.

Indian Response Strategy:
- **Military modernization and strengthening alliances** to counter China's influence.
    - Increased defense spending, partnerships with the US, Japan, and others.
- **Countering terrorism emanating from Pakistan** through various measures.
    - Strengthening border security, diplomatic efforts, and targeted operations.

Case Studies:
- **Doklam standoff (2017) and Galwan Valley clash (2020)** highlight tensions with China.
    - These incidents demonstrate the potential for escalation along the disputed border.
- **Mumbai attacks (2008) and Uri attack (2016)** underscore the threat from Pakistan.
    - Terrorist attacks with links to Pakistan-based groups highlight the security challenge.

Over-Ground Workers (OGWs)

1. Historical Context:
- **OGWs have historically supported** various insurgent and separatist movements.
- **Their role evolved** as these movements adapted to changing security landscapes.

2. Current Strategic Relationship:
- **OGWs maintain complex relationships** with both non-state and state actors.
    - Their role can vary depending on the specific conflict or group they support.

3. Areas of Cooperation:
- **No direct cooperation exists** between OGWs and security agencies.
    - OGWs operate clandestinely, supporting non-state actors.

4. Areas of Conflict:
- **OGWs facilitate terrorist activities**, posing a significant challenge to India's security.
    - They provide logistical support, recruitment, and propaganda dissemination.

5. Economic Implications:
- **OGWs can disrupt economic activities**, particularly in conflict-affected regions.
    - Extortion, intimidation, and support for activities that harm local economies.

6. Security Implications:
- **OGWs act as a force multiplier** for terrorist and insurgent groups.
    - They enable these groups to operate more effectively and evade security forces.

7. Indian Response Strategy:
- **Intelligence gathering and surveillance** to identify and disrupt OGW networks.
    - Efforts to track financial flows and communication channels.
- **Legal measures** to prosecute OGWs for their support of illegal activities.
    - The Unlawful Activities (Prevention) Act (UAPA) is a key tool.

- **Community engagement** to counter radicalization and gain support against OGWs.
    - Promoting awareness and encouraging cooperation with local populations.

8. Case Studies:
- **The arrest and prosecution of individuals** providing logistical support to terrorist groups.
- **Investigations revealing financial networks** funneling funds to insurgent organizations.

Religious & Ethnic Groups

1. Historical Context:
- **Religious and ethnic tensions** have been a persistent challenge in India's history.
    - Partition and subsequent communal violence.
- **Separatist movements** based on ethnic identity, e.g., in Northeast India.
    - Demand for autonomy or independence from India.

2. Current Strategic Relationship:
- **Complex and dynamic relationship** with the Indian state and society.
    - Some groups engage in peaceful advocacy, while others resort to violence.

3. Areas of Cooperation:
- **Government efforts to promote interfaith dialogue** and address grievances.
    - Commissions and committees to investigate communal incidents.
- **Civil society organizations** working to build bridges between communities.
    - Promoting understanding and addressing social inequalities.

4. Areas of Conflict:
- **Communal violence**, often triggered by religious or ethnic tensions.
    - Riots and targeted attacks against specific communities.
- **Insurgency and terrorism** driven by separatist or extremist ideologies.
    - Groups operating in Kashmir, Northeast India, and other regions.

5. Economic Implications:
- **Communal violence disrupts economic activity** and affects livelihoods.
    - Damage to property, loss of business, and displacement of people.
- **Conflict-affected regions** often face underdevelopment and poverty.
    - Limited investment, unemployment, and social unrest.

6. Security Implications:
- **Threat to internal stability and national unity**.
    - Undermining social cohesion and trust between communities.
- **Strain on law enforcement and security agencies**.
    - Deployment of forces and resources to maintain order.

7. Indian Response Strategy:
- **Law enforcement measures** to prevent and control violence.
    - Deployment of police, paramilitary forces, and the army in some cases.
- **Legal framework** to address terrorism and communal violence.
    - Unlawful Activities (Prevention) Act (UAPA) and other laws.
- **Political dialogue and negotiations** with some groups.
    - Peace accords and autonomy arrangements in certain regions.

8. Case Studies:
- **Anti-Sikh riots (1984) and Gujarat riots (2002)**.
    - Examples of large-scale communal violence.
- **Insurgency in Kashmir and Northeast India**.

    - Protracted conflicts involving ethnic and religious groups.

Role of Non-State Actors in Creating Challenges to Internal Security: Maritime Pirates

1. Historical Context:

- **Piracy in the Indian Ocean** has been a problem for centuries.
    - Preying on trade routes and coastal communities.

2. Current Strategic Relationship:

- **Maritime pirates operate independently** of state control.
    - They exploit gaps in maritime security and governance.

3. Areas of Cooperation:

- **No cooperation exists** between maritime pirates and states.
    - Piracy is a transnational crime, challenging international law enforcement.

4. Areas of Conflict:

- **Piracy disrupts shipping lanes**, impacting global trade.
    - Attacks on vessels and crews, leading to economic losses.
- **Piracy often involves violence** and hostage-taking.
    - Posing a threat to the safety of seafarers and maritime security.

5. Economic Implications:

- **Piracy increases shipping costs**, affecting global trade.
    - Insurance premiums, security measures, and rerouting of vessels.
- **Coastal communities can be impacted** by piracy.
    - Loss of fishing grounds, tourism revenue, and economic instability.

6. Security Implications:

- **Piracy undermines maritime security**, challenging state sovereignty.
    - Requires naval deployments, law enforcement efforts, and international cooperation.
- **Piracy can be linked to other criminal activities**.
    - Smuggling, arms trafficking, and terrorism financing.

7. Indian Response Strategy:

- **Indian Navy plays a key role** in counter-piracy operations.
    - Patrolling the Indian Ocean, escorting vessels, and deterring attacks.
- **India participates in international efforts** to combat piracy.
    - Cooperation with naval forces, intelligence sharing, and legal frameworks.
- **The Indian Coast Guard** safeguards coastal security.
    - Protecting ports, territorial waters, and critical infrastructure.

8. Case Studies:

- **Increased piracy in the Indian Ocean**, particularly off the Somali coast.
    - Led to international naval deployments and anti-piracy measures.
- **India's role in combating piracy** in the Gulf of Aden.
    - Contributing to multinational task forces and protecting Indian vessels.

Cross-Cutting Themes

Radicalization:

- **Factors contributing to radicalization** are complex and interconnected.
    - Socioeconomic inequalities, political grievances, and ideological influences.
- **External actors can exploit vulnerabilities** to spread extremist ideologies.
    - Propaganda, recruitment networks, and financial support.
- **The internet and social media** are powerful tools for radicalization.

    - Online forums, chat groups, and propaganda materials.
- **Lone-wolf attacks** are a growing concern for security agencies.
    - Individuals inspired by online propaganda.
- **Countering radicalization** requires a multi-pronged approach.
    - Addressing root causes, community engagement, and law enforcement.

Economic Security:

- **External economic shocks** can impact internal stability.
    - Global financial crises, energy price fluctuations, and supply chain disruptions.
- **Economic grievances** can fuel social unrest and radicalization.
    - Unemployment, poverty, and inequality.
- **Protecting economic interests** is a key aspect of national security.
    - Ensuring energy security, protecting critical infrastructure, and promoting economic growth.

Border Management:

- **Porous borders** pose challenges to internal security.
    - Facilitating illegal immigration, smuggling, and terrorism.
- **Effective border management** requires a multi-agency approach.
    - Cooperation between border guards, customs officials, and intelligence agencies.
- **Technological solutions** can enhance border security.
    - Surveillance systems, biometric identification, and data analytics.
- **International cooperation** is essential for effective border control.
    - Information sharing, joint operations, and capacity building.

Regional Stability:

- **Instability in neighboring countries** can spill over borders.
    - Conflict, terrorism, and organized crime.
- **Promoting regional stability** is crucial for internal security.
    - Diplomacy, development assistance, and security cooperation.
- **Regional organizations** play a role in addressing shared threats.
    - ASEAN, SAARC, and the African Union.
- **India's regional engagement** seeks to foster stability and cooperation.
    - Neighborhood First policy, Act East policy, and participation in regional forums.

Immediate Neighbors

1. Pakistan:

- **Pakistan supports terrorist groups** targeting India.
    - LeT, Jaish-e-Mohammed
- **Terror funding flows into India from Pakistan.**
    - Through various channels, including Hawala.
- **CPEC raises concerns for India's security.**
    - Passes through Pakistan-occupied Kashmir.

2. China:

- **China engages in border transgressions with India.**
    - Galwan clash in 2020
- **China's economic corridors encircle India.**
    - String of Pearls strategy
- **China supports Pakistan's stance on Kashmir.**
    - Blocking India's efforts in the UN

3. Sri Lanka:

- **Sri Lanka's Tamil issue impacts India's security.**

    - Refugee flows and potential for LTTE resurgence.
- **Sri Lanka's strategic location** attracts external powers.
    - Chinese investments in Hambantota port
- **India provides developmental aid to Sri Lanka.**
    - To counter Chinese influence.

Extended Neighbors

- India's extended neighborhood includes regions beyond its immediate borders, encompassing countries in the Indian Ocean Region, Central Asia, and Southeast Asia. These regions are of strategic importance to India's security and economic interests.

Indian Ocean Region:

- **Piracy remains a threat** in the Indian Ocean, impacting shipping and trade.
    - Attacks on vessels and crews, disrupting supply chains.
- **India has deployed naval assets** to counter piracy and protect its interests.
    - Patrolling sea lanes, escorting vessels, and participating in multinational efforts.
- **Maritime security cooperation** is crucial to address piracy and other threats.
    - Information sharing, joint exercises, and capacity building with regional partners.

Central Asia:

- **Central Asia is rich in strategic resources** that are important for India's energy security.
    - Oil, natural gas, and uranium.
- **Trade routes through Central Asia** connect India to markets in Europe and the Middle East.
    - International North-South Transport Corridor.
- **Instability in Central Asia** can impact India's security and economic interests.
    - Terrorism, extremism, and drug trafficking.

Southeast Asia:

- **Southeast Asia is a key trading partner** for India and a hub for global commerce.
    - ASEAN is India's fourth-largest trading partner.
- **India has strategic partnerships** with Southeast Asian countries.
    - Act East policy aims to strengthen economic and security ties.
- **India's engagement in Southeast Asia** seeks to promote regional stability and counter China's influence.
    - Participating in regional forums, such as ASEAN and the East Asia Summit.

China-Pakistan Economic Corridor (CPEC)

1. Strategic Implications:

- **CPEC enhances China's strategic influence** in the region.
    - Securing access to the Indian Ocean.

2. Economic Impact:

- **CPEC aims to boost Pakistan's economy**, but its sustainability is debated.
    - High debt burden and potential for Chinese dominance.

3. Security Challenges:

- **CPEC passes through Pakistan-occupied Kashmir (PoK).**
    - Raising concerns for India's territorial integrity.
- **CPEC increases Chinese military presence** in the region.
    - Security personnel deployed to protect Chinese assets.
- **CPEC could facilitate** terrorist activities targeting India.
    - Using the corridor for movement and logistics.

4. Indian Response:

- **India opposes CPEC** due to its concerns over sovereignty and security.
    - Boycotting Belt and Road Initiative forums.
- **India seeks to develop alternative connectivity projects.**
    - Chabahar Port in Iran and International North-South Transport Corridor.
- **India strengthens its military presence** along the border with Pakistan.
    - Deploying additional troops and enhancing infrastructure.

5. Future Scenarios:

- **CPEC's completion could alter the regional balance of power.**
    - Strengthening the China-Pakistan axis.
- **CPEC's success depends on various factors**, including security and economic viability.
    - Potential for instability and regional tensions.
- **CPEC will continue to be** a source of friction between India and China.
    - Impacting bilateral relations and regional dynamics.

Radicalization

1. Root Causes:

- **Socio-economic grievances** can fuel radicalization, especially among marginalized groups.
    - Poverty, unemployment, and lack of opportunities.
- **Political factors**, such as conflicts and foreign policy decisions, can contribute to radicalization.
    - Intervention in Afghanistan and global power competition.
- **Religious extremism and intolerance** can exploit vulnerabilities and promote radical ideologies.
    - Jihadi-Salafi ideology and the concept of militant jihad.
- **Psychological factors**, including alienation and a sense of belonging, play a role.
    - Seeking identity and purpose within radical groups.

2. Vulnerable Groups:

- **Youth are particularly susceptible** to radicalization due to their idealism and search for identity.
    - Recruitment efforts targeting young people online.
- **Individuals with a history of trauma** or mental health issues may be more vulnerable.
    - Exploiting feelings of anger, isolation, and resentment.
- **Marginalized communities facing discrimination** or social exclusion can be targeted.
    - Economic disparities and lack of integration.
- **Prisoners** can become radicalized while incarcerated, posing a threat upon release.
    - Extremist networks and ideologies spreading within prisons.

3. Prevention Strategies:

- **Countering extremist propaganda** online and offline is crucial.
    - Promoting alternative narratives and critical thinking skills.
- **Addressing socio-economic grievances** and promoting inclusivity is essential.
    - Providing opportunities for education, employment, and social integration.
- **Engaging community leaders** and religious figures to counter radical narratives.
    - Promoting interfaith dialogue and tolerance.
- **Strengthening border security** to prevent the flow of foreign fighters and extremist materials.
    - Collaboration with neighboring countries and international organizations.
- **Early intervention programs** to identify and support individuals at risk of radicalization.
    - Family counseling, mentoring, and psychological support.

4. Deradicalization Programs:

- **Rehabilitation programs** for individuals who have been involved in extremist activities.
    - Providing psychological counseling, vocational training, and reintegration support.
- **Disengagement programs** to help individuals leave extremist groups.
    - Addressing their ideological beliefs and offering alternative pathways.
- **Countering narratives** used by extremist groups.
    - Providing factual information and promoting critical thinking.
- **Working with families** and communities to support deradicalization efforts.
    - Providing guidance and resources to help loved ones disengage.

5. International Best Practices:

- **Sharing information and intelligence** among countries to track and counter terrorist threats.
    - Cooperation between intelligence agencies, law enforcement, and security forces.
- **Developing and implementing** comprehensive counterterrorism strategies that address the root causes of radicalization.
    - Collaboration between governments, civil society, and international organizations.
- **Promoting international legal frameworks** to combat terrorism and transnational crime.
    - UN Global Counter-Terrorism Strategy.
- **Providing capacity building** and technical assistance to countries to strengthen their counterterrorism capabilities.
    - Training programs, equipment, and financial support.

Maritime Security

- **Piracy poses significant challenges** to maritime security, impacting trade and coastal communities.
    - Piracy apprehensions rose 20% in the Indian Ocean.
    - Somalia lacks a navy and relies on international forces for support.
- **International cooperation is crucial** to counter piracy effectively.
    - UNCLOS provides legal framework for combating piracy.
    - International naval forces contribute to anti-piracy operations.
- **The Indian Navy plays a vital role** in safeguarding maritime security and trade routes.
    - The Indian Navy ensures the security of sea lanes.
    - Deploying warships, aircraft, and participating in joint exercises.
    - The Indian Navy freed 17 crew members by forcing 35 Somali pirates to surrender.
- **Piracy impacts the economy** by disrupting supply chains and increasing shipping costs.
    - Threatens maritime trade, which constitutes a significant portion of India's economy.
    - Increased insurance premiums and security measures.
- **Strategic solutions are needed to address** the root causes of piracy.
    - A robust anti-piracy law and apprehension mechanism are crucial.
    - Addressing poverty, lack of governance, and alternative livelihoods in affected regions.

Recent Cases (Post-2020)

- **The Taliban's return to power in Afghanistan in 2021** has raised concerns about regional instability and potential spillover effects on India's security.
    - The Taliban's return raises concerns about a resurgence of terrorist groups.
    - The Taliban's victory could embolden extremist groups in the region.
- **Sri Lanka's economic crisis** has highlighted the vulnerabilities of small states and the potential for external actors to exploit such situations.
    - The crisis led to political instability and protests, raising concerns about regional security.

    - China's growing influence in Sri Lanka through investments and loans has raised concerns about its strategic implications.
- **Border clashes with China in 2020** have underscored the challenges of managing a complex and contested border.
    - The clashes resulted in casualties on both sides and heightened tensions.
    - The Line of Actual Control (LAC) remains tense, with both sides increasing military presence.
    - The Cabinet Committee on Security recently approved 7 new ITBP battalions.
- **Terror attacks continue to pose a threat** to India's internal security.
    - Lone wolf attacks are rising in several Western countries and India.
    - The National Security Guard (NSG) was created to combat terrorism in 1984.
    - Terrorists are increasingly resorting to lone wolf attacks against security forces in Kashmir.
    - The NIA arrested 36 radicalized IS supporters in 2016.
    - State police arrested 18 IS supporters.
    - **Prevention efforts include strengthening anti-terrorism laws**, enhancing intelligence capabilities, and promoting counter-radicalization initiatives.
        - India has strengthened anti-terrorism laws by amending the Unlawful Activities (Prevention) Act (UAPA), 1967.
        - The NIA Act has been amended.
        - The Ministry of Home Affairs maintains a Counter Terrorism and Counter Radicalization division.
        - The Unlawful Activities (Prevention) Amendment Act of 2019 expands the scope of terror entities.
    - **India focuses on international cooperation** to combat terrorism.
        - India has proposed a permanent secretariat to coordinate efforts against terror funding.
        - India seeks to designate individuals involved in terror attacks on Indian soil as global terrorists under UNSC Resolution 1267.

Historical Cases

- **LTTE in Sri Lanka** posed significant challenges to regional security and had spillover effects on India.
    - India's intervention in the Sri Lankan Civil War (1987-1990) through the Indian Peace Keeping Force (IPKF).
- **Kargil War (1999)** was a direct military confrontation with Pakistan that highlighted the challenges of border management and the risks of infiltration.
    - Intelligence failures were identified as a contributing factor to the conflict. (*IDSA Task Force Report*)
    - The Kargil Review Committee recommended reforms in intelligence coordination. (*IDSA Task Force Report*)
- **Mumbai 26/11 Attacks (2008)** demonstrated the vulnerability of India to transnational terrorism and the use of maritime routes for attacks.
    - Intelligence lapses and lack of preparedness were identified as key issues.
    - The attacks highlighted the need for enhanced coastal security and counter-terrorism capabilities.
- **Operation Cactus (1988)** involved India's military intervention in the Maldives to thwart a coup attempt and restore the legitimate government.
    - It showcased India's role as a regional security provider.

Internal Security **1**
Constitutional Framework 1
Article 355: Union's Duty to Protect States 1
Emergency Provisions 1
Institutional Architecture 2
Intelligence Agencies: IB, R&AW, NIA 2
Investigation Agencies, Coordination Mechanisms, and Jurisdiction 2
Legislative Framework 3
Regular Laws (IPC, CrPC) 3
Bharatiya Nyaya Sanhita, 2023 3
The Bharatiya Nyaya Sanhita, 2023 3
Special security legislation (UAPA, NIA Act) 4
NATGRID 5
Emergency Laws (AFSPA) 5
Recent Amendments and Their Impact 6
Traditional Challenges Cluster 6
Terrorism and Insurgency 6
Left Wing Extremism 6
Border Security 6
Maritime Security 7
Island Territory Protection 7
Emerging Challenges Cluster 8
Cyber Security 8
Mob Violence 8
Drug Trafficking 8
Money Laundering 8
Environmental Security Threats 9
Preventive Measures 9
Intelligence Gathering 9
Interagency Coordination 9
Community Policing 10
Border Management 10
Cyber Security Framework 10
Reactive Measures 11
Crisis Response Protocols 11
Hot Pursuit Doctrine 11
Surgical Strikes 11
Disaster Management 12
Post-Incident Investigation 12
When Studying AFSPA 12
Constitutional Aspects (Article 355) 12
Security Requirements (Army's Perspective) 13
Human Rights Concerns (Supreme Court Views) 13
International Standards (UN Guidelines) 13
Recent Developments (Areas Under AFSPA) 14
Unlawful Activities (Prevention) Act (UAPA): 14
Case Study Integration 15
Historical Cases 15

1. Punjab Crisis (1980s)....15
2. Mumbai Attacks (26/11, 2008)....15
3. URI Surgical Strikes (2016)....16
Contemporary Cases....16
1. Recent Cyber Attacks....16
2. Cross-Border Terrorism Incidents....16
3. Successful Anti-Terror Operations....16
Comparative Cases....16
1. International Best Practices....16
2. Other Countries' Security Frameworks....17
3. Global Cooperation Mechanisms....17
Dutch Coastguard:....17

Internal Security

Constitutional Framework

Article 355: Union's Duty to Protect States

Main Points:

- **Article 355: Constitutional mandate for the Union to protect states against external aggression and internal disturbances.**
  - Empowers Union to ensure states' territorial integrity and internal order.
- **Union's duty extends to situations where state governments are unable to maintain law and order.**
  - Intervention can occur when states request assistance or in exceptional circumstances.
- **Article 355 empowers the Union to deploy armed forces, paramilitary forces, and intelligence agencies.**
  - It enables deployment of resources to assist state authorities in restoring stability.
- **Article 355 invoked in situations like insurgency, terrorism, communal violence, and natural disasters.**
  - It provides a constitutional basis for intervention in various situations affecting internal security.
- **Deployment of security forces under Article 355 subject to judicial review.**
  - Safeguards against arbitrary use of power and ensures accountability of the Union government.
- **Cooperation and coordination between Union and state governments are crucial for the effective implementation of Article 355.**
  - Mechanisms for information sharing, joint operations, and capacity building are important.

Emergency Provisions

Main Points:

- **Indian Constitution provides for three types of emergencies: National, State, and Financial.**
  - Articles 352, 356, and 360 respectively
- **National Emergency (Article 352): Proclaimed during war, external aggression, or armed rebellion.**
  - Affects the entire country, centralizes power, and restricts fundamental rights.
- **State Emergency (Article 356): Imposed when a state government fails to function according to the Constitution.**
  - Also known as President's Rule; Union government assumes control of the state.

- **Financial Emergency (Article 360): Declared in situations of economic crisis or financial instability.**
    - Empowers Union to control financial affairs and reduce salaries of government employees.
- **Emergency provisions intended to safeguard the sovereignty, unity, and integrity of India.**
    - Allows for extraordinary measures to deal with exceptional circumstances.
- **Parliamentary and judicial oversight mechanisms exist to ensure accountability during emergencies.**
    - Parliament approves and can revoke emergency declarations; courts can review their validity.
- **Emergency provisions debated for potential misuse and impact on federalism and democracy.**
    - Safeguards are in place to prevent abuse of power and protect citizens' rights.
- **Amendments to emergency provisions have aimed at addressing concerns and ensuring greater transparency.**
    - 44th Amendment requires the President to act on the advice of the Cabinet.

Institutional Architecture

Intelligence Agencies: IB, R&AW, NIA

Main Points:

- **Intelligence Bureau (IB): India's oldest intelligence agency, responsible for internal security and counterintelligence.**
    - IB technically falls under the Ministry of Home Affairs.
    - IB's VIP security unit is responsible for the safety of VIPs.
- **Research and Analysis Wing (R&AW): India's external intelligence agency, responsible for gathering foreign intelligence.**
    - Experts say R&AW's role has varied under different prime ministers.
    - R&AW claims to have contributed to the creation of Bangladesh in 1971.
- **National Investigation Agency (NIA): A specialized agency for investigating terrorism-related offenses.**
    - NIA cases are assigned by the central government.
    - The NIA Act was amended in 2019 to strengthen anti-terrorism laws.
- **Intelligence agencies need a clear legal framework for their existence and functioning.**
    - Their functioning must be under parliamentary oversight.
- **Reforms needed in recruitment and training to attract the best talent.**
    - Intelligence agencies should have the flexibility to "hire and fire".
- **Coordination among intelligence agencies is crucial for effective intelligence gathering and analysis.**
    - The National Security Council (NSC) and its substructures play a role in intelligence coordination.

Investigation Agencies, Coordination Mechanisms, and Jurisdiction

- **Central Bureau of Investigation (CBI): India's premier investigating agency, handling a wide range of criminal cases.**
    - CBI is under the jurisdiction of the Ministry of Personnel, Public Grievances and Pensions
- **Enforcement Directorate (ED): Responsible for enforcing economic laws and investigating financial crimes.**
    - ED is under the Department of Revenue, Ministry of Finance
- **Directorate of Revenue Intelligence (DRI): Focuses on combating smuggling and customs fraud.**
    - DRI is an Indian intelligence agency; its apex body is the Central Board of Indirect Taxes and Customs

- **Multi Agency Centre (MAC): A platform for intelligence sharing and coordination among various security and intelligence agencies.**
    - MAC is under the Intelligence Bureau (IB), Ministry of Home Affairs
- **Jurisdictional overlaps and interoperability issues can sometimes hinder effective coordination among these agencies.**
    - Lack of clarity in roles and responsibilities, competition for resources, and differing operational procedures can pose challenges.
- **Streamlining procedures, establishing clear protocols, and fostering inter-agency trust are crucial for enhancing coordination.**
    - This can include joint training exercises, sharing of best practices, and establishing mechanisms for real-time information exchange.

Legislative Framework

Regular Laws (IPC, CrPC)

- **The Indian Penal Code (IPC) defines various offenses and prescribes punishments.**
    - It covers offenses against the state, public tranquility, and individuals ([Bharatiya Nyaya Sanhita, 2023]).
- **The Criminal Procedure Code (CrPC) lays down the procedures for investigation, trial, and sentencing of criminal offenses.**
    - It ensures fair trial, due process, and protection of rights of accused persons ([Bharatiya Nagarik Suraksha Sanhita, 2023]).
- **Regular laws provide a framework for law enforcement agencies to maintain law and order.**
    - They empower the police to investigate crimes, apprehend suspects, and gather evidence ([Bharatiya Nagarik Suraksha Sanhita, 2023]).
- **Courts play a crucial role in adjudicating criminal cases and delivering justice.**
    - They ensure the rule of law and protect fundamental rights ([Bharatiya Nagarik Suraksha Sanhita, 2023]).
- **The IPC and CrPC are regularly amended to address emerging security challenges and evolving criminal tactics.**
    - Recent amendments have focused on terrorism, cybercrime, and organized crime ([Bharatiya Nyaya Sanhita, 2023], [Bharatiya Nagarik Suraksha Sanhita, 2023]).
- **Effective implementation of regular laws is essential for maintaining internal security and upholding the rule of law.**
    - Police reforms, judicial efficiency, and public awareness are crucial for strengthening the justice system ([Bharatiya Nyaya Sanhita, 2023], [Bharatiya Nagarik Suraksha Sanhita, 2023]).

Bharatiya Nyaya Sanhita, 2023

Mentions several chapters that cover offenses against the state, public tranquility, and individuals:

- **Chapter VI: Of Offences against the State** covers offenses such as waging war against the Government of India and sedition
- **Chapter XI: Of Offences against the Public Tranquility** includes offenses like unlawful assembly, rioting, and promoting enmity between different groups
- **Chapters XVII and XVIII: Of Offenses Against Property and Of Offenses Affecting the Human Body** encompass a wide array of offenses against individuals, including theft, robbery, assault, and murder

The *Bharatiya Nyaya Sanhita, 2023*

Lists the following sections within **Chapter XI: Of Offences against the Public Tranquility**:

- **Section 187: Unlawful assembly** defines the concept of an unlawful assembly and outlines various scenarios that constitute this offense

- **Section 188: Every member of the unlawful assembly guilty of the offense committed in prosecution of common object** establishes the culpability of each participant in an unlawful assembly for offenses carried out in pursuit of their shared objective
- **Section 189: Rioting** defines the offense of rioting, which involves violence and disturbance of the peace by an unlawful assembly
- **Section 190: Wantonly giving provocation with intent to cause riot—if rioting is committed; if not committed** addresses the act of deliberately provoking a riot and outlines the punishments based on whether a riot actually occurs
- **Section 191: Liability of owner, occupier, etc., of land on which an unlawful assembly or riot takes place** establishes the responsibility of property owners or occupiers for unlawful assemblies or riots that take place on their land
- **Section 192: Affray** defines the offense of affray, which involves fighting in a public place that disturbs the peace
- **Section 193: Assaulting or obstructing public servant when suppressing riot, etc.** deals with the offense of attacking or hindering a public servant who is attempting to quell a riot or other public disturbance
- **Section 194: Promoting enmity between different groups on the ground of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony** addresses actions that incite hatred or discord between different groups based on various factors and harm societal harmony
- **Section 195: Imputations, assertions prejudicial to national integration** covers acts that involve making statements or spreading information that undermines national unity and integrity

Important sections include:

- Section 145: This section defines the punishment for waging war against the Government of India. It includes attempting to wage war or abetting the waging of war. The punishment is death, life imprisonment, or a fine.
- Section 146: This section covers conspiracy to commit offenses punishable under Section 145.
- Section 147: This section addresses the act of collecting arms with the intention of waging war against the Government of India.
- Section 148: This section deals with concealing with intent to facilitate a design to wage war.
- Section 149: This section makes it an offense to assault the President, Governor, etc., with the intent to compel or restrain the exercise of any lawful power.
- Section 150: This section focuses on acts that endanger the sovereignty, unity, and integrity of India.

Special security legislation (UAPA, NIA Act)

- **Unlawful Activities (Prevention) Act (UAPA), 1967:** Amended in 2019 to strengthen anti-terrorism laws.
    - Allows designation of individuals as terrorists.
    - Grants NIA officers authority to seize property without DGP approval.
- **National Investigation Agency (NIA) Act, 2008:** Establishes the NIA as a specialized agency to combat terrorism.
    - Investigates scheduled offenses, including terrorism-related cases.
    - Can receive cases from the Central Government.
    - Aims to be a highly trained, partnership-oriented workforce.
- **Amendments post 26/11 Mumbai attacks:** Coastal security arrangements reviewed and strengthened.
    - 12 Coast Guard districts established along with Air Enclaves.
    - Indian Navy focuses on secure sea lanes and freedom to use the seas.
- **Challenges to internal security:** Proxy wars, misuse of internet, and terrorist funding.
    - Foreign countries support insurgent groups, impacting national security.

    - Non-state actors use internet and social media for subversive activities.
    - Lack of global consensus on terrorism hinders effective counter-terrorism efforts.
- **Recommendations for combating terrorism:** Need for political consensus, good governance, and socioeconomic development.
    - Strengthen police force, improve prosecution, and leverage NATGRID.
    - Address issues of radicalization and terrorist funding.
- **Intelligence reforms:** Focus on capability improvement, inter-agency coordination, and parliamentary oversight.
    - Need for a clear legal framework for intelligence agencies.
    - Establishment of a National Intelligence Coordinator (NIC) or Minister for National Security.
    - Parliamentary oversight committee for policy, administrative, and financial matters.

NATGRID

NATGRID, or the **National Intelligence Grid**, is an integrated intelligence master database structure in India. It is intended for counter-terrorism purposes by connecting databases of core security agencies under the Government of India. It aims to collect comprehensive patterns from 21 different organizations and make them accessible to security agencies around the clock. NATGRID was created after the 2008 Mumbai attacks exposed weaknesses in India's intelligence networks and is part of an overhaul of the country's security and intelligence systems.
Some key features of NATGRID include:

- **Data sources:** NATGRID will have access to data from immigration entry and exit, banking and financial transactions, credit card purchases, telecom, individual taxpayers, air flyers, and train travelers. This data will be used to generate intelligence inputs.
- **Connected agencies:** 11 user agencies will have real-time access to NATGRID data, including:
    - Intelligence Bureau (IB)
    - Research & Analysis Wing (R&AW)
    - National Investigation Agency (NIA)
    - Central Bureau of Investigation (CBI)
    - Enforcement Directorate (ED)
    - Directorate of Revenue Intelligence (DRI)
    - Financial Intelligence Unit (FIU)
    - Central Board of Direct Taxes (CBDT)
    - Central Board of Excise and Customs (CBEC)
    - Directorate General of Central Excise and Intelligence (DGCEI)
    - Narcotics Control Bureau (NCB)
- **Purpose:** NATGRID will help security agencies identify, capture, and prosecute terrorists and preempt terror plots. It will also enable agencies to locate information on terror suspects from various organizations and services.

NATGRID is meant to be a tool to enhance counter-terrorism efforts, but it has also faced controversy due to concerns about:

- **Federal structure:** Some argue that NATGRID infringes on the federal structure because police is a state subject.
- **Access limitations:** The efficacy of NATGRID in preventing terror has been questioned since no state agency or police force can access its database.
- **Data protection:** There have been calls for statutory backing for NATGRID with safeguards for data protection.

Despite these controversies, NATGRID has signed an MoU with the National Crime Records Bureau (NCRB) for access to the centralized online database on FIRs and stolen vehicles. This will give NATGRID access to the Crime and Criminal Tracking Network and Systems (CCTNS), a platform that links around 14,000 police stations. As of December 31, 2020, NATGRID is reported to be operational under the Home Ministry.

Emergency Laws (AFSPA)

- **Armed Forces (Special Powers) Act (AFSPA), 1958:** Empowers armed forces to maintain public order in disturbed areas.
    - Grants special powers like arrest without warrant and use of force.
    - Need for thorough investigation into complaints of misuse or abuse of powers.
- **Supreme Court directives on AFSPA usage (NPMHR v. India, 1997):** Guidelines for armed forces to prevent misuse.
    - Operations restricted to declared 'Disturbed Areas'.
    - Only designated officers can exercise powers of arrest and use of force.

Recent Amendments and Their Impact

- **UAPA Amendment (2019):** Strengthens anti-terrorism laws and expands the definition of terrorist activities.
    - **Individuals can be designated as terrorists** by the government.
    - **NIA officers can seize property** without DGP approval.
- **NIA Amendment (2019):** Empowers NIA to investigate crimes related to counterfeit currency and human trafficking.
    - **Sessions Courts can be designated as Special Courts** to expedite trials.
- **Constitution (One Hundredth Amendment) Act, 2015:** Deals with the exchange of territories between India and Bangladesh.
- **Constitution (Application to Jammu and Kashmir) Order, 2019:** Revokes Article 370, impacting J&K's special status.

Traditional Challenges Cluster

Terrorism and Insurgency

- **Hinterland Jihadi Terrorism:** Exists outside of Jammu & Kashmir, posing challenges for intelligence agencies.
    - Concerns about online radicalisation via internet and social media platforms.
    - Need to go beyond strategic and law enforcement approaches.
- **Community involvement crucial in counter-terrorism:** Family reporting suspicious activity to NIA.
- **India faces various forms of terror:** Requires a country-specific strategy.
    - Ethno-nationalist, religious, Left Wing Extremism (LWE), and narco-terrorism.
- **Countering Violent Extremism (CVE):** Focus on prevention and community-based efforts to counter radicalisation.
    - **US model:** Efforts to prevent recruitment and address underlying ideologies and grievances.
    - **Need for India-specific CVE policy:** Considering diverse religious and socio-political landscape.
- **Global Counterterrorism Forum (GCTF):** Focuses on capacity building and international cooperation.
- **AQIS threat to India:** Targets security forces and right-wing Hindu organizations.
    - Establishment of Ansar Ghazwat-ul-Hind (AGH) in Kashmir with al-Hurr media wing.
- **Kashmir insurgency:** Driven by ISI interference, communal conflict, and socio-economic issues.
    - Use of social media for radicalisation and inciting violence.

Left Wing Extremism

- **Naxalism:** Significant internal security challenge, particularly in tribal areas.
    - **Government's multi-pronged approach:** Security, public perception management, development, and rehabilitation.
    - **Integrated Action Plan (IAP):** Flagship program with significant financial resources.

- **Andhra Pradesh model:** Combines military tactics with surrender and rehabilitation packages.
- **Challenges for security forces:** Operational philosophy, mindset, willingness, and resources.
    - Need for clarity on central and state government roles and responsibilities.
    - **Technological solutions:** Drones to minimize casualties among security personnel.
- **Factors contributing to LWE:** Socio-political structures challenged via violent revolution.

Border Security

- **Coastal security:** Vulnerability highlighted after the 26/11 Mumbai attacks.
    - **Coastal Security Exercises:** Conducted by the Indian Navy (IN) and Coast Guard.
    - **Importance of secure sea lanes:** For trade and national interests.
- **Assam Rifles:** Role in border security and counter-insurgency operations.
    - **Dual control structure:** Operational control under the army, administrative under the Home Ministry.
    - The Assam Rifles comprises 46 battalions. Of these, 20 are involved in guarding the India-Myanmar border and 26 battalions are involved in counter-insurgency roles, including two in Jammu and Kashmir.
    - **Proposed merger with ITBP:** Raises concerns about border vigil with China.
- **ITBP:** Secures Indo-China and Indo-Myanmar borders during peace and war.
    - **Security of sensitive installations:** Including Rumtek Monastery and LBSNAA.
    - The Indo-Tibetan Border Police (ITBP) Force was raised on 24 October, 1962. At present, the ITBP guards 3,488 km long India-China borders ranging from the Karakoram Pass in Ladakh to Jachep La in Arunachal Pradesh. Apart from this, the Force also has important roles in many internal security duties and operations against the Left Wing Extremism in the state of Chhattisgarh.
- **Special Frontier Force (SFF):** Covert paramilitary unit controlled by R&AW.
    - **Recruitment:** Initially Tibetan exiles, now a mix of Tibetans and Gorkhas.
    - **Role:** Protecting the nation from internal and external threats.
- **Line of Actual Control (LAC):** Tension with China and increased infrastructure build-up.
    - **ITBP's role:** Ensuring border security and defensive preparedness.

The **Integrated Action Plan (IAP)** is a flagship program launched by the Indian government to address the challenges of **Left Wing Extremism (LWE)**, also known as Naxalism. The IAP focuses on a multi-pronged approach that includes security measures, efforts to manage public perception, development initiatives, and rehabilitation programs for affected areas. The program involves significant financial resources, exceeding INR 6000 crore annually. The IAP aims to tackle the complex socio-political and economic factors contributing to LWE, striving to improve living conditions and reduce the appeal of extremist ideologies in affected regions.

Maritime Security

- **India's vast coastline and maritime interests:** Require robust security measures to protect trade and resources.
    - **12 major ports and 200 minor ports** contribute significantly to India's economy.
- **26/11 Mumbai attacks exposed vulnerabilities:** Highlighted the need for enhanced coastal security.
    - **Indian Navy and Coast Guard conduct Coastal Security Exercises** to improve preparedness.
- **Securing Sea Lanes of Communication (SLOCs):** Crucial for India's energy security and trade.
    - **Indian Navy's maritime strategy** focuses on ensuring secure SLOCs.
- **Countering maritime piracy:** A growing concern in the Indian Ocean Region, impacting international trade and security.

Island Territory Protection

- **Andaman and Nicobar Islands:** Strategically important, requiring dedicated security arrangements.
    - **National Security Guard (NSG) hub in Gandhinagar** extends its reach for counter-terrorism operations.
    - **Two Coast Guard districts** dedicated to the region for maritime security.
- **Lakshadweep and Minicoy Islands:** Vulnerable to security threats due to their remote location.
    - **Coast Guard district in Kavaratti** responsible for security and surveillance.
- **Protection of Exclusive Economic Zone (EEZ):** Safeguarding resources and economic interests.
    - **Indian Navy initiatives contribute to security in the EEZ.**

Emerging Challenges Cluster

Cyber Security

- **Communication networks vital for national security:** Disruptions have major implications for India's stability.
    - **Defined as Critical Information Infrastructure (CII)** under IT Act 2000.
- **Cyberattacks pose serious threats to CII:** Targeting individuals, businesses, and government entities.
    - **Types include phishing, malware, DDoS attacks, and ransomware.**
    - **"WannaCry" ransomware attack (2017) affected 150 countries.**
- **State and non-state actors exploit cyberspace:** For espionage, sabotage, and political influence.
    - **Dark web, AI-enabled tools used for fake news, recruitment, radicalisation.**
    - **Lack of global norms allows targeting of CII.**
- **5G technology presents opportunities and risks:** Enhanced connectivity but potential for increased vulnerabilities.
    - **Higher speeds and data capacity** necessitate robust security measures.
- **Jurisdictional challenges hinder cybersecurity:** Subject not specifically listed in the 7th Schedule.
    - **Opposition from state governments** over federalism concerns.
- **Government initiatives to strengthen cybersecurity:** Establishing agencies and implementing strategies.
    - **National Critical Information Infrastructure Protection Centre (NCIIPC).**
    - **National Counter Ransomware Task Force.**
    - **Indian Computer Emergency Response Team (CERT-In).**
- **Recommendations for enhancing cybersecurity:** Awareness, international cooperation, and AI integration.
    - **Stricter regulations, improved incident response systems, and public-private partnerships.**

Mob Violence

- **Social media fuels mob violence:** Spread of misinformation and incitement to violence.
    - **Rumors and fake news used to instigate youth.**
- **Stone pelting incidents in Kashmir:** Example of radicalized youth targeting security forces.

Drug Trafficking

- **Drug trafficking poses a multifaceted security threat:** Affects health, fuels crime, and undermines governance.
    - Narco-terrorism, especially in Northwest India, creates illegal trafficking zones.
- **India's location makes it vulnerable:** Situated between major drug producing regions (Golden Triangle & Golden Crescent).

- **Porous borders exploited by trafficking networks:** For smuggling drugs into and through India.
- **Drug money used to finance terrorist activities:** Threatens national security and stability.

Money Laundering

- **Money laundering conceals illicit funds:** Makes it difficult to trace proceeds of crime and prosecute offenders.
- **Hawala and other informal channels used:** To move money across borders, bypassing formal financial systems.
    - *India has proposed a permanent secretariat to coordinate the fight against terror funding.*
- **Shell companies and fictitious transactions:** Often used to disguise the origin and destination of illegal funds.
- **Money laundering undermines financial integrity:** Erodes trust in the system and facilitates other criminal activities.

Environmental Security Threats

- **Environmental degradation impacts security:** Resource scarcity, climate change, and natural disasters can lead to conflicts.
    - The NSC is mandated to address security threats in the area of ecology.
- **Water disputes between states and countries:** Competition for water resources can escalate tensions and instability.
- **Climate change exacerbates existing vulnerabilities:** Displacement, migration, and competition for resources can lead to social unrest.
- **Deforestation and illegal wildlife trade:** Contributes to environmental damage and weakens ecosystems.
- **Government initiatives for environmental protection:** Policies and programs to address climate change and promote sustainable development.
    - The widening of charters is advocated to include environmental security.

Preventive Measures

Intelligence Gathering

- **Enhance Human Intelligence (HUMINT) capabilities**: To gather actionable insights on emerging threats.
    - Focus on **recruiting personnel with language proficiency** and local knowledge.
- **Improve Technical Intelligence (TECHINT) infrastructure**: Utilize technology for effective surveillance and data analysis.
    - Invest in **advanced monitoring tools, data analytics, and AI capabilities** for predictive intelligence.
- **Develop robust open-source intelligence gathering**: Leverage publicly available information for threat assessment.
    - Train analysts to **extract valuable insights from social media, news reports, and academic publications.**
- **Address counter-intelligence lapses**: Strengthen measures to prevent leaks and infiltration of intelligence agencies.
    - Enforce stricter **vetting procedures, background checks, and internal monitoring systems.**

Interagency Coordination

- **Establish a National Intelligence Coordinator (NIC)**: To oversee and coordinate intelligence agencies' activities.
    - Task Force on National Security recommends the appointment of an **intelligence czar**.

- **Strengthen the National Security Council (NSC) System**: Improve information sharing and policy integration.
    - Enhance the **NSC Secretariat's role in intelligence assessment and coordination**.
- **Formalize information exchange mechanisms**: Promote seamless communication between agencies.
    - Implement **secure communication platforms** and joint training programs for personnel.
- **Clearly define roles and responsibilities**: Avoid overlaps and ensure efficient allocation of resources.
    - Conduct periodic **reviews of interagency cooperation** and address any gaps or challenges.

Community Policing

- **Build trust between police and communities**: Encourage dialogue and collaboration to address local concerns.
    - Organize **community meetings, workshops, and awareness campaigns** to foster understanding.
- **Empower local communities to participate**: Involve citizens in crime prevention and reporting.
    - Establish **neighbourhood watch programs, youth groups, and citizen advisory boards.**
- **Train police officers in community engagement**: Equip them with skills to handle diverse perspectives and sensitivities.
    - Emphasize **conflict resolution, cultural awareness, and sensitivity training** for police personnel.
- **Promote community-based initiatives**: To address social issues that contribute to crime and violence.
    - Support **youth programs, employment opportunities, and social welfare initiatives** in vulnerable areas.

Border Management

- **Strengthen border infrastructure and surveillance**: Deploy technology and manpower for effective monitoring.
    - Invest in **modern fencing, sensor networks, drones, and patrol boats.**
- **Enhance coordination between border security forces**: Improve communication and joint operations.
    - Establish **joint command centers** and conduct regular **joint exercises and training programs.**
- **Improve intelligence gathering and sharing**: Identify and disrupt trafficking networks and cross-border criminal activities.
    - Develop **cross-border intelligence-sharing mechanisms** with neighboring countries.
- **Address socio-economic factors**: In border regions that contribute to vulnerabilities and illegal activities.
    - Promote **economic development, education, and infrastructure** in border communities.

Cyber Security Framework

- **Develop a comprehensive national cyber security strategy**: Define clear objectives, roles, and responsibilities.
    - Establish a **central authority** to oversee implementation and coordinate efforts.
- **Strengthen critical information infrastructure protection**: Implement robust security measures for vital systems.

    - Mandate **regular security audits, vulnerability assessments, and incident response plans.**
- **Promote public-private partnerships**: Leverage expertise and resources from the private sector.
    - Establish **joint task forces** and **information-sharing platforms** for collaboration.
- **Enhance cyber awareness and education**: Train individuals and organizations on cyber threats and preventive measures.
    - Integrate **cybersecurity education** in school curricula and conduct **public awareness campaigns.**

An **intelligence czar** is a high-ranking official responsible for overseeing and coordinating the activities of a country's intelligence agencies. The Task Force on National Security in India has recommended the appointment of an intelligence czar to address concerns regarding coordination between agencies.
The intelligence czar concept aims to streamline intelligence operations by:

- **Improving communication and information sharing** between different agencies.
- **Reducing duplication of efforts** and ensuring efficient use of resources.
- **Providing a single point of contact** for the government on intelligence matters.

Proponents of the intelligence czar model argue it would enhance national security by facilitating a more cohesive and effective intelligence apparatus.

Reactive Measures

Crisis Response Protocols

- **Clearly defined roles and responsibilities**: For various agencies involved in crisis management.
    - **National Crisis Management Committee (NCMC)** to coordinate responses.
- **Effective communication and coordination**: Ensure seamless flow of information during a crisis.
    - Utilize **secure communication channels** and establish **joint operation centers.**
- **Rapid deployment of forces**: To contain the situation and minimize casualties.
    - Develop **pre-positioned forces** and **quick reaction teams (QRTs)** for immediate response.
- **Standardized operating procedures (SOPs)**: To guide actions and ensure consistency in response.
    - Develop SOPs for **various types of crises**, including terrorist attacks, natural disasters, and pandemics.
- **Regular drills and exercises**: To test preparedness and identify areas for improvement.
    - Conduct **simulations and tabletop exercises** involving all relevant agencies.

Hot Pursuit Doctrine

- **Allows security forces to cross borders**: To pursue and apprehend perpetrators who flee after committing an act of aggression.
    - Requires **prior consent or agreements with neighboring countries.**
- **Legal and operational complexities**: Careful consideration needed to avoid violating international law.
    - Establish **clear rules of engagement** and ensure **accountability for actions taken.**
- **Effective communication and coordination**: With neighboring countries essential for successful implementation.
    - Establish **joint mechanisms** for information sharing and coordination during hot pursuit operations.
- **Potential for escalation and miscalculation**: Risk of triggering conflicts with neighboring countries.
    - Use hot pursuit **judiciously** and as a **last resort** when other options have been exhausted.

- **Strengthening border security**: To minimize the need for hot pursuit operations.
    - Focus on **deterrence, surveillance, and intelligence gathering** to prevent cross-border infiltration.

Surgical Strikes

- **Pre-emptive military operations**: Targeting specific enemy installations or individuals to neutralize threats.
    - Carried out with **precision and speed** to minimize collateral damage.
- **Demonstration of capability and resolve**: Sends a strong message of deterrence to adversaries.
- **Operational planning and execution**: Requires meticulous intelligence gathering and coordination between agencies.
    - Ensure **clear objectives, target selection, and well-defined exit strategies.**
- **Risk of escalation and unintended consequences**: Surgical strikes can trigger retaliatory attacks and heighten tensions.
    - Conduct **thorough risk assessments** and consider **potential diplomatic ramifications.**
- **Post-strike communication and diplomacy**: Essential to manage international perceptions and prevent escalation.
    - Communicate **objectives clearly** and engage in **diplomatic efforts to de-escalate tensions.**

Disaster Management

- **Comprehensive Disaster Management Plan**: For all potential hazards - natural and man-made.
    - Conduct vulnerability assessments and risk mapping exercises.
- **Early Warning Systems**: Provide timely and accurate alerts to minimize impact.
    - Invest in weather forecasting, seismic monitoring, and communication infrastructure.
- **Preparedness and Capacity Building**: Train first responders, establish evacuation procedures, and stockpile essential supplies.
    - Conduct regular drills and exercises, involve communities in disaster preparedness efforts.
- **Rapid Response and Relief**: Deploy rescue teams, provide medical aid, and restore critical infrastructure.
    - Establish clear command and control structures, coordinate with NGOs and international agencies for assistance.
- **Rehabilitation and Reconstruction**: Focus on long-term recovery and build back better.
    - Address housing, livelihood, and infrastructure needs, incorporate disaster resilience in reconstruction efforts.

Post-Incident Investigation

- **Securing the Scene**: Preserve evidence, prevent contamination, and ensure safety of personnel.
    - Establish a cordon, document the scene, collect physical evidence.
- **Witness Interviews**: Gather eyewitness accounts and statements from those involved.
    - Conduct interviews promptly, use trained investigators, follow legal procedures.
- **Forensic Analysis**: Examine physical evidence, digital footprints, and other relevant materials.
    - Utilize specialized laboratories, analyze DNA, ballistics, and other forensic data.
- **Reconstruction of Events**: Establish a timeline, identify key actors, and determine the sequence of events.
    - Analyze witness statements, forensic evidence, and other relevant data.
- **Reporting and Recommendations**: Prepare a detailed report with findings, conclusions, and recommendations.

    - Identify lessons learned, suggest improvements to response mechanisms, share findings with relevant agencies.

Note: The National Security Guard (NSG) is a specialized force trained in counter-terrorism and anti-hijacking operations. The NSG also performs bomb disposal, post-blast investigation, and hostage rescue. These skills can be valuable in post-incident investigations related to security incidents, including terrorist attacks.

When Studying AFSPA

Constitutional Aspects (Article 355)

- Empowers the Union to protect states against external aggression and internal disturbance. This forms the basis for deploying armed forces in disturbed areas.
    - AFSPA enables the Union to fulfill its duty to ensure the security and stability of states. (Constitution of India)
- Reflects the principle of federalism, where the Union government intervenes to assist states facing challenges to internal security.
    - The Union can act upon a state's request or independently when necessary. (Constitution of India)
- Balances the need for security with the protection of individual rights and freedoms.
    - AFSPA has been criticized for granting excessive powers to the armed forces.
- Subject to judicial review to ensure compliance with constitutional principles.
    - Supreme Court judgments have placed limitations on the use of AFSPA.
- Essential for maintaining the integrity and sovereignty of the nation.
    - AFSPA provides a legal framework for countering threats to internal security.

Security Requirements (Army's Perspective)

- Provides necessary legal protection for soldiers operating in hostile environments.
    - AFSPA shields soldiers from prosecution for actions taken in good faith during counter-insurgency operations.
- Enables swift and decisive action against insurgents and terrorists, ensuring the safety of civilians.
    - AFSPA empowers the army to conduct searches, arrests, and use force when necessary to maintain order.
- Crucial for maintaining the morale and operational effectiveness of the armed forces in challenging situations.
    - AFSPA provides a clear legal framework for soldiers operating in complex and dangerous environments.
- Effective tool for countering insurgency and restoring peace in disturbed areas.
    - Army officials argue that AFSPA is essential for tackling insurgency and terrorism.
- Requires clear rules of engagement and accountability mechanisms to prevent misuse.
    - The army has implemented guidelines and training programs to ensure responsible use of AFSPA powers.

Human Rights Concerns (Supreme Court Views)

- Granting special powers to armed forces can lead to human rights violations and impunity.
    - Concerns have been raised about extrajudicial killings, torture, and arbitrary detentions in areas under AFSPA.
- Importance of upholding fundamental rights even in conflict zones.
    - Supreme Court has emphasized the need to balance security requirements with the protection of human rights.
- Need for robust oversight mechanisms to ensure accountability for actions taken by armed forces.
    - Supreme Court has directed that complaints of human rights violations should be thoroughly investigated.

- Emphasis on the principle of proportionality in the use of force.
    - Force used by armed forces must be proportionate to the threat and should minimize harm to civilians.
- Need to review and amend AFSPA to address human rights concerns and ensure compliance with international standards.
    - Supreme Court has recommended safeguards to prevent misuse of AFSPA and protect human rights.

International Standards (UN Guidelines)

- States have a duty to protect human rights, including in situations of armed conflict or internal disturbance.
    - International human rights law sets standards for the conduct of armed forces.
- Use of force by law enforcement agencies must be guided by principles of necessity, proportionality, and accountability.
    - UN Basic Principles on the Use of Force and Firearms by Law Enforcement Officials provide guidance on lawful use of force.
- Importance of independent investigations into allegations of human rights violations.
    - UN Special Rapporteurs and human rights organizations have called for investigations into alleged abuses in areas under AFSPA.
- Need for transparency and access to justice for victims of human rights violations.
    - International human rights mechanisms provide avenues for redress and accountability.
- Promoting dialogue and reconciliation to address the root causes of conflict and instability.
    - UN has emphasized the importance of addressing underlying grievances and promoting peaceful resolution of conflicts.

Recent Developments (Areas Under AFSPA)

- Partial revocation of AFSPA from certain areas based on improved security situations.
    - The government has been gradually reducing the areas under AFSPA.
- Ongoing debates and discussions on the need for further amendments or repeal of the act.
    - Civil society groups and human rights organizations continue to advocate for repeal of AFSPA.
- Efforts to enhance training and oversight mechanisms to prevent misuse of AFSPA.
    - The government has implemented measures to improve training and accountability of armed forces.
- Challenges in balancing security imperatives with the protection of human rights.
    - Finding a balance between addressing security threats and safeguarding human rights remains a challenge.
- Emphasis on a holistic approach to counter-insurgency, including development and addressing grievances.
    - The government has recognized the need for a multi-pronged strategy to address the root causes of insurgency.

Unlawful Activities (Prevention) Act (UAPA):

The **UAPA**, enacted in 1967, is a crucial law for **countering terrorism** and **unlawful activities** in India. It has undergone several amendments to address evolving security challenges and concerns regarding human rights.

Key Sections and Provisions:

- **Section 15(1)(b) of the UAPA**: Defines a "terrorist act" and includes acts committed under nine listed treaties.
- **Schedule to the Act:** Lists nine treaties, including the Convention for the Suppression of Terrorist Bombings (1997) and the Convention against Taking of Hostages (1979).
- **2019 Amendment**: Introduces security features to define high-quality counterfeit Indian currency notes, including watermarks.

Amendments and Developments:

- **UAPA Amendment Act, 2019:** Addresses various issues related to combating terrorism and strengthens the NIA's powers.
- **Expansion of Terror Entities**: Empowers the government to designate individuals as terrorists, in addition to organizations, if they prepare, commit, participate in, promote, or are involved in terrorism.
- **Approval for Seizure of Property**: Requires NIA officers to obtain approval from the Director General of NIA to seize properties connected with terrorism.
- **Empowering NIA**: Allows NIA officers of the rank of Inspector or above to investigate terrorism cases.
- **Inclusion of International Convention**: Adds the International Convention for Suppression of Acts of Nuclear Terrorism (2005) to the list of treaties defining terrorist acts.

Data and Case Studies:

- **Usman Case**: Highlights the lack of maritime piracy-specific legislation, leading to the use of UAPA for prosecution.
- **Challenges in Punishing Piracy**: The 2019 amendment aims to address this issue by bringing piracy and related activities under its ambit.

Recommendations and Concerns:

- **Need for Maritime Piracy Legislation**: The Usman case demonstrates the gap in legal provisions for maritime piracy.
- **Coordination Among Agencies**: Effective coordination among agencies involved in capturing, transporting, and prosecuting pirates is crucial.
- **Safeguards Against Misuse**: Concerns regarding potential misuse of UAPA's broad powers require robust oversight mechanisms and safeguards to protect individual rights.

The **Usman Case**, also known as *The State of Maharashtra v. Usman Salad & Others* (2011), involved the arrest and trial of 15 Somali pirates in India. The case exposed **the lack of specific legislation in India to address maritime piracy**. As a result, the prosecution had to rely on the **Unlawful Activities (Prevention) Act (UAPA),** along with other general penal statutes, to charge the accused.

The case highlighted several key issues:

- The absence of a dedicated maritime piracy law meant the act of piracy itself remained technically unpunished, even though the accused were convicted on other charges.
- Difficulties in securing the testimony of foreign witnesses, crucial in piracy cases, as exemplified by the failure of Thai and Myanmar crew members to appear in court.
- A significant delay in trial proceedings, with the Usman case taking almost six years to reach a verdict.
- Challenges in evidence collection, highlighting a lack of coordination between agencies like the Indian Navy, which conducted the anti-piracy operation, and the Mumbai police, responsible for the investigation.

The Usman case served as a critical example of the legal and procedural complexities involved in prosecuting maritime piracy in India. It ultimately contributed to the push for developing comprehensive legislation specifically addressing this crime.

Case Study Integration

Historical Cases

1. Punjab Crisis (1980s)

- **Originated from socio-political factors**: Demands for greater autonomy and Sikh identity assertion.
    - Economic disparities and perceived discrimination fueled resentment
- **Escalated into violent insurgency**: Led by militant groups demanding Khalistan.
    - Operation Blue Star (1984) aimed to flush out militants from the Golden Temple
- **Government response involved military operations**: Also included political negotiations and social outreach.
    - Punjab Accord (1985) aimed to address some grievances, but militancy persisted

- **Crisis had significant impact**: On national security, social fabric, and human rights.
    - Thousands of lives lost, widespread human rights violations, and displacement occurred

2. Mumbai Attacks (26/11, 2008)

- **Series of coordinated terrorist attacks**: Carried out by Lashkar-e-Taiba (LeT), targeting multiple locations in Mumbai
    - Exploited vulnerabilities in coastal security, highlighting intelligence and preparedness gaps
- **Security forces responded**: National Security Guard (NSG) deployed for counter-terrorism operations
    - Delayed response time and lack of coordination among agencies hampered effectiveness
- **Attacks exposed systemic flaws**: In India's security apparatus, prompting calls for comprehensive reforms
    - Led to enhanced coastal security measures, intelligence sharing, and counter-terrorism capabilities.

3. URI Surgical Strikes (2016)

- **Cross-border operation conducted by Indian Army**: In response to a terrorist attack on an army base in Uri, Jammu and Kashmir
    - Aimed to preemptively target terrorist launchpads across the Line of Control (LoC)
- **Signaled a shift in India's counter-terrorism policy**: Towards a proactive and offensive approach
    - Demonstrated the use of strategic and tactical intelligence for precision strikes
- **Generated mixed reactions**: From international community, with some concerns about escalation
    - Reinforced India's resolve to combat terrorism and protect its national security interests

Contemporary Cases

1. Recent Cyber Attacks

- **Targeting critical infrastructure**: Including financial institutions and government networks.
    - **DDoS Attacks**: Overwhelm servers with traffic, causing service disruptions.
    - **Ransomware attacks**: Encrypt data, demanding payment for decryption.
- **State and non-state actors involved**: Cyber warfare, espionage, and criminal activities.
    - **WannaCry virus**: Impacted computers globally, demanding Bitcoin ransom.
- **Government response**: Enhanced cybersecurity measures, international cooperation.
    - **National Counter Ransomware Task Force**: Established to address ransomware threats.
    - **CERT-In**: National agency for cybersecurity incident response and support.

2. Cross-Border Terrorism Incidents

- **Infiltration and attacks**: Terrorists exploiting porous borders to launch attacks.
    - **Uri attack (2016)**: Terrorist attack on an Indian Army base.
- **State-sponsored terrorism**: Foreign powers using terrorist groups as proxies.
    - **Challenges to designation**: China blocking India's attempts to designate individuals as terrorists at the UN.
- **Government response**: Strengthening border security, intelligence gathering.
    - **Surgical strikes (2016)**: Proactive cross-border operation targeting terrorist camps.
    - **Strengthening anti-terror laws**: Amendments to the UAPA.

3. Successful Anti-Terror Operations

- **Neutralizing terrorist threats**: Preempting attacks, apprehending terrorists.

    - **National Security Guard (NSG)**: Special forces unit for counter-terrorism and hostage rescue.
    - **Black Cats**: NSG commandos known for their expertise and efficiency.
- **Intelligence-led operations**: Gathering actionable intelligence to disrupt terrorist activities.
    - **Importance of community involvement**: Identifying and reporting suspicious activities.
- **International cooperation**: Sharing intelligence, joint operations.
    - **Global Counterterrorism Forum**: Promoting international cooperation against terrorism.

Comparative Cases

1. International Best Practices

- **Community-based CVE programs:** Engaging local communities to prevent radicalization.
    - **US Department of Homeland Security**: Implements partnerships with faith leaders and communities.
- **Clear legal frameworks for intelligence agencies**: Ensuring accountability and oversight.
    - **Parliamentary oversight mechanisms**: Scrutinizing intelligence agencies' activities.
- **Focus on intelligence coordination and integration**: Sharing information among agencies.
    - **National Intelligence Councils**: Provide strategic analysis and coordinate intelligence efforts.

2. Other Countries' Security Frameworks

- **Integrated security strategies**: Addressing both internal and external security threats.
    - **EU Internal Security Strategy**: Defines common challenges and promotes cooperation among member states.
- **Civilian-military cooperation**: Integrating civilian and military capabilities for security operations.
    - **Dutch Coastguard**: Example of successful integration of civilian and military elements.
- **Cybersecurity strategies**: Protecting critical infrastructure from cyber threats.
    - **Belgium's Cyber Security Strategy**: Focuses on protecting critical networks and systems.

3. Global Cooperation Mechanisms

- **Intelligence sharing and joint operations**: Counterterrorism efforts require international collaboration.
    - **INTERPOL**: Facilitates global police cooperation and information exchange.
    - **Europol**: EU agency for law enforcement cooperation, supporting member states in fighting crime and terrorism.
- **Countering terrorist financing**: International efforts to disrupt funding sources for terrorist groups.
    - **Financial Action Task Force (FATF)**: Sets international standards to combat money laundering and terrorist financing.
- **Capacity building and technical assistance**: Supporting developing countries in strengthening their security capabilities.
    - **Global Counterterrorism Forum (GCTF)**: Focuses on capacity building and countering violent extremism.

Dutch Coastguard:

- The **Dutch Coastguard Centre** is located at the naval base in Den Helder.
- It has an **integrated staff** that includes both **military and civilian personnel**.
- Assets like aircraft and helicopters operate under the responsibility of different ministries, and **pilots are often military personnel** on active service.

North East Insurgencies 1
Historical Background: Colonial Legacy 1
Post-independence integration challenges in North East India: 2
Early separatist movements and their causes 3
Strategic location sharing borders with multiple countries 3
Chicken's neck corridor significance 4
Terrain and its impact on insurgency 5
Major Insurgency Movements 5
1) Naga Movement: 5
2) Mizo Insurgency: 6
3) ULFA in Assam: 6
4) Bodo Movement: 7
5) Tripura Insurgency: 7
6) Recent Developments: 7
Peace Accords and Settlements 8
1) Shillong Accord (1975): 8
2) Mizoram Accord (1986): 8
3) Assam Accord: 9
4) Bodo Accord: 9
5) Recent Peace Initiatives 10
Government Response Framework 11
1) Military Operations: 11
2) Development Initiatives: 11
3) Political Solutions: 12
4) Constitutional Provisions: 13
Current Challenges and Way Forward 13
1) Economic Development Issues: 13
2) Cultural Preservation Concerns: 14
3) Cross-border challenges: 15
4) Integration efforts: 16

North East Insurgencies

Historical Background: Colonial Legacy

- **British Colonial Frontier Making:** The **Inner Line Permit (ILP)**, a concrete example of colonial frontier policy, **restricted movement** into hill areas, directly impacting the **Naga, Mizo, and other tribal groups**
    - The **ILP** created a physical and administrative separation, impacting **trade routes** and **access to resources** for communities in the hills
    - The **North East Frontier Tract (NEFT)**, carved out of Assam, is a specific example of how the British formalized the division between hill and plain regions
    - The **McMahon Line**, drawn without local consultation, remains a point of contention and contributes to regional instability
- **Colonial Political Economy:** The establishment of **tea plantations in Assam** led to the **displacement of indigenous populations** like the **Bodo and Ahom**, creating a legacy of land alienation
    - **Resource exploitation** focused on tea and timber, **benefiting the British** while leaving the region underdeveloped. The lack of investment in local industries is a continuing grievance
    - The **monopoly over salt trade** by the British disrupted the traditional economy and led to resentment among many groups in the northeast.

    - **Limited trade and economic linkages** between the Northeast and rest of India, a direct result of colonial policies, continue to impact the region
- **Colonial Social and Cultural Impacts:** The imposition of a **uniform education system** in the Northeast, neglecting local languages and cultural practices, is a prime example of colonial cultural impact
    - **Christian missionary activity** altered the religious landscape and sometimes led to conflicts with traditional belief systems, such as in the case of the **Naga** and **Mizo** people
    - **Ethnic tensions** were exacerbated by British policies, such as the use of **different administrative systems** for various ethnic groups, as was the case with the **Kuki** and **Naga** tribes
    - The **introduction of new legal systems** clashed with existing community-based justice systems and undermined local authority structures.
- **Anti-Colonial Resistance:** The **Kuki Rebellion (1917-1919)** in Manipur is a concrete example of armed resistance against the British, showcasing the tribal groups' fight for self-determination
    - The **Mizo National Front (MNF)** movement's initial armed struggle and later negotiations that led to the Mizoram Accord is an important example of resistance to colonial legacy
    - **Non-cooperation movements** in the plains regions of Assam also showed resistance to British rule.
    - The legacy of these movements fueled **post-colonial insurgencies** and continues to shape political discourse in the region.
- **Post-Colonial Challenges:** The **failure to integrate the Northeast into the Indian political mainstream** after independence, coupled with the unresolved issues of land ownership from colonial times, further fueled discontent
    - **Influx of immigrants**, particularly from Bangladesh, created resource pressures and ethnic tensions, exemplified by the **Bodo-Muslim conflict** in Assam
    - **Underdevelopment** and lack of economic opportunities continues to be a key grievance across the region. **Poor infrastructure and limited access to education** are some of the consequences .
    - The **Armed Forces Special Powers Act (AFSPA)**, implemented in response to insurgencies, remains a controversial example of a post-colonial challenge, due to alleged human rights violations and restrictions on freedom.

Post-independence integration challenges in North East India:

- **Geographical isolation** due to the 1947 partition created integration challenges.
    - A narrow Siliguri corridor connects the region to the rest of India.
- **Diverse ethnic groups** with unique cultures caused conflicts and integration issues.
    - Over 125 distinct tribal groups exist in the region.
    - These groups have clashed over land, resources, and representation.
- **Historical grievances** and demands for autonomy fueled insurgencies in the region.
    - Insurgencies have demanded greater autonomy to complete independence.
- **Socio-economic factors** such as poverty, unemployment, and lack of development contributed to unrest.
    - The region is industrially backward with weak infrastructure.
- **Political marginalization** and a lack of representation led to resentment.
    - Tribal origins and appearance put people against the federal system.
- **Porous international borders** and the easy availability of arms intensified conflicts.
    - The region shares borders with Bangladesh, Bhutan, Myanmar and China.
- **Influx of illegal migrants** and border control issues created additional challenges.
    - Radical Assamese nationalism was fueled by illegal migration post-1947.
- **Lack of infrastructure** and connectivity hampered economic integration.
    - The region has weak infrastructure making it difficult for integration.
- **Limited governance** and a weak system of land records posed challenges.

    - Absence of formal land records prevents access to loans.
- **Security forces violations** caused alienation and a sense of injustice.
    - Deep sense of alienation exists due to human rights violations.
- **The 'look-east' policy** sought to integrate the region but had security implications.
    - The policy aimed to leverage the region's strategic location and resources.
- **The region's complex history** under British colonial rule added to these issues.
    - The British created an imperial frontier and segregated the hills.
- **The Armed Forces Special Powers Act** was used with many human rights concerns.
    - Commission recommended repealing it and incorporating provisions in the UAPA.
- **The region's diverse tribal groups** often seek local autonomy.
    - There are more than 125 distinct tribal groups in the North East.
- **Insurgents often run a parallel government** influencing decisions of local authorities.
    - Militant organizations have been known to operate this way in the North East.
- **The region is rich in natural resources** but struggles with development.
    - North East has huge natural resources like oil, gas, coal, and fertile land.
- **The North East has a mix of ethno-nationalist, religious, and Left-Wing extremism**.
    - These movements have different goals and reasons.
- **Regional disparities** have grown, causing competition among North East states.
    - There is a potential for conflicts to rise due to intra-regional disparities.
- **The region's population growth** has stressed livelihoods and land fragmentation.
    - Population growth exceeded 200% between 1951 and 2001.
- **Corruption** and other issues of local governance continue to pose problems.
    - ULFA recruitment grew due to corruption, and government failures.
- **The North East Council (NEC)** was set up to coordinate development in the region.
    - NEC was established to provide inter-state coordination.
- **The Ministry of Development of North Eastern Region (DONER)** and NEC's roles have overlapped.
    - Public opinion is that DONER has compromised NEC's efficacy.

Early separatist movements and their causes

- **Emergence of Separatist Sentiments:** The Northeast region saw early separatist movements driven by distinct socio-political factors and ethnic identities.
    - The Naga and Mizo insurgencies arose as early expressions of self-determination.
    - These movements sought greater autonomy or complete independence from India.
- **Historical Grievances:** The region's unique historical context significantly fueled early separatist tendencies.
    - British colonial policies resulted in a loosely administered frontier zone, fostering alienation.
    - The Inner Line Regulation of 1873 segregated hill populace from the plains, impacting integration.
- **Ethnic and Cultural Identity:** Strong ethnic and tribal identities played a crucial role in separatist movements.
    - Each community sought to preserve its unique culture and traditions, and was wary of external influence.
    - The diverse tribal groups, such as the **Nyishis** of Arunachal, had long histories of autonomy.
- **Socio-Economic Factors:** Underdevelopment and economic disparities were major catalysts for early insurgencies.
    - The region's perceived neglect by the central government led to resentment.
    - Unemployment and lack of economic opportunities contributed to the rise of insurgent groups.
- **Geographical Isolation and Connectivity:** The region's geographical isolation further exacerbated separatist sentiments.
    - The narrow Siliguri Corridor created a sense of disconnect from the Indian mainland.

    - Porous international borders facilitated external support for insurgent groups.
- **Influence of External Support:** External support from neighboring countries aided the early separatist movements.
    - China and Myanmar have been implicated in providing support to insurgents.
    - The availability of arms across the porous borders further fueled these movements.
- **Demand for Greater Nagalim:** The **NSCN (IM)** aimed for a "Greater Nagalim" incorporating Naga-inhabited areas, escalating tensions.
    - This demand included parts of Assam, Arunachal, Manipur, and Myanmar, causing regional concerns.
    - The Nagaland Assembly has endorsed this integration multiple times, reflecting deep-seated aspirations.

Strategic location sharing borders with multiple countries

- **Extensive International Borders:** The Northeast shares a vast international border, making it a crucial and sensitive region for India.
    - It accounts for about **40% of India's land borders** with neighboring countries.
    - The region is surrounded by Bangladesh, Bhutan, Myanmar, and China.
- **Gateway to Southeast Asia:** The region acts as a vital bridge connecting India with the vibrant economies of Southeast Asia.
    - Its strategic location is pivotal for India's "Act East Policy" initiatives.
    - The region's connectivity is essential for regional cooperation and economic integration.
- **Geographic Vulnerabilities:** The region's unique geography creates vulnerabilities and security challenges.
    - The **narrow Siliguri Corridor** is a critical link to the rest of India, but also a point of weakness.
    - Porous borders facilitate the movement of insurgents, arms, and illicit goods.
- **Complex Security Dynamics:** The presence of multiple international borders complicates internal security management.
    - Cross-border activities of insurgent groups are a significant security concern.
    - External actors may provide support to these groups, exacerbating the situation.
- **Strategic Importance in National Defense:** The Northeast is a vital part of India's defense architecture, requiring significant attention and resources.
    - The region's location necessitates strong security measures to safeguard national interests.
    - Infrastructure development along the borders is crucial for defense preparedness.
- **Economic and Resource Hub:** The region is endowed with substantial natural resources, making it economically significant.
    - It possesses oil, gas, coal, hydro-power, and fertile land.
- This economic potential is crucial for national development and regional prosperity.
- **Historical Significance:** The region's history of being a frontier zone during British rule contributes to its present strategic importance.
    - Colonial policies created a distinct identity, leading to integration challenges.
    - Understanding this history is critical for addressing current issues and promoting integration.

Chicken's neck corridor significance

- **Vital Link:** The Siliguri Corridor, also known as the "Chicken's Neck," is a crucial and narrow strip of land connecting the Northeast to the rest of India.
    - It is approximately **22 sq km** wide at its narrowest point, making it a strategic choke point.
    - This corridor is essential for transportation, communication and supply lines to the North East.
- **Geographical Vulnerability**: The narrowness of the corridor makes it highly vulnerable to disruptions and security threats.

    - Its small size makes it susceptible to blockade or military action, jeopardizing access to the region.
    - The corridor's **proximity to international borders** adds to its strategic sensitivity.
- **Strategic Importance:** The corridor's security is paramount for maintaining India's territorial integrity and access to the Northeast.
    - It serves as the sole land route for connecting the Northeast to the Indian mainland.
    - Any disruption in the corridor can severely impact the region's economy, security, and governance.
- **Defense and Security**: The corridor is a vital element in India's defense architecture, requiring robust security measures.
    - Its protection is essential for ensuring the seamless movement of military personnel and equipment.
    - The presence of security forces like the ITBP is critical for maintaining stability in the area.
- **Economic Significance**: The corridor facilitates trade and economic activities between the Northeast and other parts of India.
    - It is a major route for transporting goods and commodities crucial for the region's economy.
    - Smooth operation of the corridor is vital for economic development and regional prosperity.
- **Historical Context**: The corridor's significance has been recognized since British colonial times due to its strategic location.
    - British policies focused on controlling this area to ensure seamless governance and trade with the North East.
    - Its historical importance underscores the necessity for its continued security.
- **Integration Challenges**: The geographical separation caused by the corridor presents integration challenges for the Northeast.
    - It creates a sense of disconnect from the mainland, which has contributed to separatist sentiments.
    - Addressing these challenges requires special attention and policy interventions for the region.

Terrain and its impact on insurgency

- **Rugged Topography**: The North East's challenging terrain, characterized by hills and dense forests, significantly impacts insurgency.
    - It provides **natural hideouts** and operational advantages for insurgent groups.
    - The difficult terrain hinders the movement and operations of security forces.
- **Dense Forest Cover:** The region's extensive forests offer cover and concealment, facilitating insurgent activities.
    - These **forests act as safe havens** and training grounds for insurgent groups.
    - The thick vegetation makes it difficult for security forces to conduct effective patrols.
- **Porous Borders:** The porous nature of the international borders, combined with difficult terrain, allows easy cross-border movement.
    - This facilitates the influx of arms, militants, and illicit goods.
    - The **long and unguarded borders** make it challenging to monitor and control movement.
- **Limited Infrastructure**: The terrain hinders the development of robust infrastructure, affecting counter-insurgency efforts.
    - Lack of roads and communication networks impedes troop movement and logistical support.
    - Underdeveloped infrastructure impacts socio-economic development, fueling discontent.
- **Accessibility Issues:** The difficult terrain and poor infrastructure result in accessibility challenges for security forces.

    - Remote areas often remain ungoverned, providing safe havens for insurgents.
    - This limits the **reach and effectiveness** of government administration and security measures.
- **Operational Challenges**: The terrain creates unique operational challenges for security forces engaged in counter-insurgency.
    - It requires specialized training and equipment for effective operations.
    - Security forces must adapt their tactics to the environment, such as using ITBP.
- **Impact on Insurgent Tactics:** Insurgent groups use the terrain to their advantage, employing guerrilla warfare tactics.
    - They use **ambushes and hit-and-run tactics**, leveraging knowledge of local terrain.
    - The challenging environment complicates counter-insurgency strategies and requires adaptive planning.

Major Insurgency Movements

1) Naga Movement:

- **Historical Grievances:** The Naga movement stems from historical grievances related to the integration of Naga areas into India following independence. The Nagas' desire for self-determination has been a central theme of the conflict.
    - **Demand for Greater Nagalim**: The Naga insurgent group, NSCN (IM), advocates for a "Greater Nagalim" encompassing Naga-inhabited areas in several Indian states and parts of Myanmar. This claim involves significant territorial disputes with Assam, Manipur, and Arunachal Pradesh.
    - The Nagaland Assembly has repeatedly endorsed the “Greater Nagalim” demand.
- **Political Autonomy:** The Naga movement seeks greater autonomy or even independence from India. This reflects a deep-seated desire for self-governance and control over their affairs.
    - The movement has witnessed several factions, causing internal conflicts within the movement.
    - The NSCN-IM's negotiations with the Indian government have yielded limited progress over decades.
- **External Influence:** External support and influence have played a role in prolonging the Naga conflict. This complicates the peace process and undermines the movement's legitimacy.
    - Some sources suggest China's potential involvement in supplying arms and support to the NSCN-IM.
    - The influence of outside actors on the movement requires close attention.

2) Mizo Insurgency:

- **Origins and Aims:** The Mizo insurgency originated from feelings of marginalization and lack of development in the Mizo Hills (present-day Mizoram). The movement aimed at achieving independence from India.
    - The Mizo National Front (MNF) was a prominent insurgent group advocating for independence.
    - The insurgency involved violence, displacement, and significant loss of life.
- **Mizoram Accord:** The Mizoram Accord of 1986 marked a significant turning point, bringing an end to the armed conflict and ushering in a period of peace in Mizoram.
    - The accord incorporated provisions for greater autonomy within the framework of the Indian Union.
    - It highlights the potential for successful conflict resolution through dialogue and negotiation.
- **Socio-Economic Factors:** Socio-economic issues like poverty, unemployment, and perceived neglect from the government have contributed to the insurgency. This reflects the link between development and conflict.
    - Addressing socio-economic disparities remains crucial for lasting peace and stability.

    - The state's unique geographical features, rich biodiversity, and cultural heritage need careful management.

3) ULFA in Assam:

- **Origins and Ideology:** The United Liberation Front of Assam (ULFA) emerged in the 1970s, advocating for an independent Assam based on Assamese nationalism. This arose from grievances related to the influx of illegal migrants from East Pakistan (Bangladesh) and perceived economic and cultural marginalization.
    - The ULFA's initial demand was for a sovereign Assam, which later evolved to include demands for greater autonomy and socio-economic reforms.
    - **Key figures:** Paresh Barua is a key figure associated with the ULFA's armed struggle.
- **Methods and Activities:** The ULFA engaged in armed rebellion, employing tactics such as ambushes, bombings, and kidnappings. This caused significant disruption and loss of life. The group is also known for its links to foreign agencies, seeking to destabilize the region.
    - The ULFA has a history of using porous borders with Myanmar for operational bases and arms supply.
    - The group's activities significantly impacted Assam's socio-political stability and economic development.
- **Current Status:** While the ULFA's strength has diminished considerably following crackdowns, it continues to pose a security challenge. Several factions exist within the ULFA, some have initiated peace talks with the government.
    - Some ULFA cadres set up transit camps and safe houses in the Manabhum Reserve Forest.
    - The group has reportedly lost considerable public support over time.

4) Bodo Movement:

- **Ethno-Nationalist Roots:** The Bodo movement is rooted in the ethno-nationalist aspirations of the Bodo people, an indigenous group inhabiting the Brahmaputra Valley in Assam. The movement reflects a desire for greater self-governance and cultural preservation.
    - The movement gained momentum in the 1980s with the formation of various insurgent groups.
    - Demand for a separate Bodo state fueled the movement.
- **Violence and Conflict:** The Bodo movement has witnessed periods of intense violence, including clashes between insurgent groups, security forces, and other communities. The conflict caused displacement, destruction, and significant loss of life.
    - The National Democratic Front of Bodoland (NDFB) was a prominent Bodo insurgent group.
    - The conflict affected socio-economic development and security situation in Assam.
- **Bodo Accord and Peace Efforts:** The Bodo Peace Accord of 2020 is a significant development, paving the way for the creation of a new territorial council. This highlights the government's efforts to resolve conflict through dialogue and negotiation.
    - The accord aims at addressing Bodo people's aspirations while maintaining the existing political system.
    - The implementation of the accord is crucial for achieving long-term peace and stability.

5) Tripura Insurgency:

- **Tribal Marginalization:** The Tripura insurgency is rooted in the marginalization and displacement of the indigenous tribal population due to demographic shifts. This has fueled demands for greater autonomy and protection of tribal rights.
    - The influx of non-tribal populations has altered the demographic landscape, leading to unrest.

    - The state has witnessed clashes between tribal and non-tribal communities, leading to violence.
- **Insurgent Groups and Activities**: Various insurgent groups like the National Liberation Front of Tripura (NLFT) and All Tripura Tiger Force (ATTF) have engaged in violence. Their objective is to seek greater autonomy or independence.
    - These groups have carried out attacks on security forces and civilians, causing instability.
    - The insurgents have also been involved in kidnappings, extortion, and other unlawful activities.
- **Peace Initiatives and Challenges**: The government has initiated peace talks and rehabilitation programs, but challenges remain. The persistent issue of displacement and socio-economic disparities continue to hinder the peace process.
    - The implementation of rehabilitation packages requires a careful balance between the needs of both tribal and non-tribal populations.
    - The long-term success of peace initiatives depends on addressing underlying issues of marginalization and identity.

6) Recent Developments:

- **Counter-Insurgency Operations**: Security forces have intensified counter-insurgency operations to curb insurgent activities across the Northeast. These operations focus on disrupting insurgent networks and maintaining law and order.
    - The use of technology and intelligence gathering has been critical in these operations.
    - These operations often raise concerns about human rights violations in affected areas.
- **Ceasefire Agreements**: Several insurgent groups have signed ceasefire agreements with the government, signaling a positive shift. The commitment of all stakeholders to maintain these agreements is crucial for lasting peace.
    - The Naga ceasefire, though ongoing, continues to be a matter of concern due to the involvement of external forces.
    - The Bodo Accord is a positive development; however, its successful implementation is vital.
- **Development and Connectivity**: The government is focusing on infrastructure and development projects to address socio-economic grievances. These are considered root causes of insurgency.
    - Initiatives like the "Act East" policy aim to integrate the Northeast with Southeast Asia, boosting trade and connectivity.
    - The North Eastern Council (NEC) is promoting regional development through various programs and projects.
- **Regional Cooperation:** Enhanced cooperation with neighboring countries is helping to address cross-border insurgent activities and arms smuggling. This also includes controlling illegal migration.
    - Coordination with Myanmar has helped in curbing the movement of insurgents and arms.
- The Multi-purpose National Identity Card (MNIC) is a measure to control illegal migration.
- **Challenges and Way Forward**: Despite progress, challenges such as ethnic tensions, unemployment, and drug trafficking persist. Addressing these issues and working towards a more inclusive and integrated approach will be important for lasting peace in the region.
    - The crime-insurgency nexus continues to pose a threat to the region.
    - Effective implementation of government policies and schemes requires coordination between central and state governments.

Peace Accords and Settlements

1) Shillong Accord (1975):

- **Context and Objectives:** The Shillong Accord aimed to bring an end to the insurgency in Nagaland, initiated by the Naga National Council (NNC). The accord was a controversial agreement that led to divisions among the Nagas.
    - The accord was signed between the Government of India and the NNC.
    - The NNC agreed to accept the Indian constitution.
- **Key Provisions:** The NNC agreed to unconditionally accept the Constitution of India. It also agreed to surrender their arms.
    - The agreement led to the formation of the Nationalist Socialist Council of Nagaland (NSCN) due to disagreement.
    - The accord faced opposition from a section of Naga leaders who viewed it as a betrayal.
- **Limitations and Impact**: The Shillong Accord did not fully resolve the Naga issue, resulting in the rise of new insurgent groups. The accord is seen as a significant factor in the continuation of the Naga conflict.
    - The accord led to the formation of the NSCN and further fragmentation of Naga society.
    - The demand for a "Greater Nagalim" remains a point of contention, extending beyond Nagaland.

2) Mizoram Accord (1986):

- **Background and Goal**: The Mizoram Accord sought to end the Mizo National Front (MNF) insurgency that had been active since the 1960s. The accord aimed to bring peace and integrate the MNF into the political mainstream.
    - The accord was signed between the Indian government and the MNF, led by Laldenga.
    - The accord was largely successful and led to the establishment of Mizoram as a state.
- **Main Terms**: The MNF agreed to cease hostilities and surrender their weapons and join the democratic process. The accord granted statehood to Mizoram.
    - The accord included provisions for rehabilitation of MNF cadres, and provided for social and economic development.
    - The accord recognized Mizo culture, language, and tradition as a marker of their identity.
- **Positive Outcomes**: The Mizoram Accord is widely considered a successful peace settlement. The accord brought long-term stability and progress in Mizoram.
    - Mizoram has since been one of the most peaceful states in the region.
    - The accord is a model for peaceful resolution of conflicts in the Northeast region.

3) Assam Accord:

- **Background and Objectives**: The Assam Accord was signed in 1985 to address the issue of illegal immigration from Bangladesh and protect the rights of indigenous Assamese people. The accord was the result of a six-year-long agitation.
    - The accord was signed between the central government and the leaders of the Assam Movement.
    - The main objective was to identify and deport illegal immigrants who entered Assam after 1971.
- **Key Provisions:** The accord stipulated that those who entered Assam after 1971 would be identified and deported. It also provided for economic development and protection of Assamese culture.
    - The accord led to the amendment of the Citizenship Act, 1955.
    - It also included measures to prevent future illegal immigration through border fencing and increased vigilance.

- **Limitations and Impact:** The implementation of the Assam Accord has faced several challenges, particularly in identifying and deporting illegal immigrants. This has led to continued social tensions and unrest in the state.
    - The issue of illegal migration remains a sensitive and contentious matter, causing ethnic conflicts.
    - The accord did not fully address the concerns of all stakeholders, contributing to the rise of new insurgent groups.

4) Bodo Accord:

- **Context and Goal:** The Bodo Accord was signed to resolve the Bodo Insurgency, which sought a separate state for the Bodo people within Assam. The accord aimed to grant more autonomy to the Bodo people.
    - The Bodo Territorial Council (BTC) was established as a result of the accord in 2003.
    - The accord aimed to foster greater political and administrative autonomy for the Bodos.
- **Main Terms:** The accord created the Bodoland Territorial Area District (BTAD) and granted it significant legislative and executive powers. It included provisions for the protection of the Bodo people's culture, language, and land rights.
    - The BTC was granted control over various subjects including land, water, and local customs.
    - The jurisdiction of the Bodoland Territorial Council embraces almost all the items in lists II and III.
- **Positive and Negative Outcomes:** The Bodo Accord has contributed to a reduction in violence and insurgency in the region. However, there have been issues regarding the implementation of certain provisions and concerns about the distribution of power.
    - There is discontent in older councils over the preferential treatment of the Bodoland Territorial Council.
    - The accord has not fully addressed all grievances and there are some lingering tensions related to land rights and resource allocation.

5) Recent Peace Initiatives

- **Government efforts** have focused on weakening the ecosystem of terror through consistent action by security forces and agencies.
    - The government is actively addressing the root causes of insurgency through developmental projects.
- **Infrastructure development** in the border areas has been ramped up, which enhances security and connectivity.
    - **India and China** are both investing heavily in military infrastructure near the Line of Actual Control (LAC).
- **SMART policing** is being implemented, emphasizing strictness, sensitivity, modernity, and accountability in law enforcement.
    - This approach aims to address the security challenges posed by Left Wing Extremism and other groups.
- **Use of technology** is increasing for better identification and prediction of digital security attacks and breaches.
    - **Artificial Intelligence** and machine learning are being used to strengthen digital security.
- **The Armed Forces Special Powers Act (AFSPA)** has been partially withdrawn from some areas of Arunachal Pradesh.
    - There are recommendations to repeal AFSPA in the North East, incorporating some provisions into the Unlawful Activities (Prevention) Act.
- **The North East Council (NEC)** is a nodal agency for the economic and social development of the North East.
    - The NEC funds projects in agriculture, industry, health, power, and tourism.

- **The North Eastern Development Finance Corporation Ltd (NEDFi)** provides financial assistance to promote industrial development in the region.
    - NEDFi aims to support the establishment of various economic ventures on commercial lines.
- **The "Act East" policy** seeks to strengthen connectivity with the ASEAN region through trade and infrastructure.
    - This policy aims to make the North East a major economic hub linking India with Southeast Asia.
- **The Multi-purpose National Identity Card (MNIC)** project aims to register citizens, which can help to deter illegal immigration.
    - The pilot project collects personal details, photographs, and biometric data for a credible ID system.
- **Capacity building** in administration and local governance is crucial to address conflicts.
    - Efforts are being made to improve the delivery of public services by entrusting responsibilities to local bodies.
- **Village self-governance** is being promoted, with village councils being established in areas under the Sixth Schedule of the constitution.
    - These initiatives aim to strengthen democratic processes at the grassroots level.
- **The North Eastern Police Academy (NEPA)** is being upgraded to train more police officers at the induction level.
    - NEPA is also being developed for civil administration training.
- **The National Register of Indian Citizens** is being updated, and this process is vital for managing migration and citizenship issues.
    - The Citizenship Act, 1955 has been amended to include a specific section on the registration of citizens.
- **Inter-state projects** in communication, education, and health care are being promoted by the NEC to foster regional cooperation.
    - These projects aim to improve connectivity, human resource development, and access to health care.

Government Response Framework

1) Military Operations:

- **Counter-insurgency operations** are conducted by security forces in the North East and other areas when deemed necessary, under army control.
    - Assam Rifles has a role in maintaining law and order in the North-Eastern areas.
- The **National Security Guard (NSG)** was raised in 1984 to combat terrorism and is a unique mix of personnel from the Army, Central Armed Police Forces and State Police Forces.
    - NSG commandos are used to neutralize terrorist threats and handle hijacking situations.
- **Special Frontier Force (SFF)** is a covert paramilitary unit controlled by R&AW and reports directly to the Cabinet Secretariat.
    - SFF was raised after the 1962 China-India war and initially recruited Tibetan exiles.
- **Combing operations** by security forces are a regular feature of counterinsurgency operations, especially in tribal areas.
    - These operations aim to maintain security in Naxal-affected regions.
- The **Armed Forces Special Powers Act (AFSPA)** was enacted in 1958 to give operational freedom to security forces in disturbed areas.
    - AFSPA has been partially withdrawn from some areas of Arunachal Pradesh.
- **Assam Rifles** was formed in 1835 to protect British tea estates and has performed conventional combat roles.
- The Assam Rifles has been involved in counter-insurgency and peacekeeping operations.
- **The Indo-Tibetan Border Police (ITBP)** plays a key role in border security, particularly along the Line of Actual Control (LAC).

    - ITBP also conducts counter-insurgency operations in Jammu and Kashmir and anti-naxal operations.
- **The Cabinet Committee on Security (CCS)** is the apex body for executive action on matters of national security.
    - The CCS coordinates the actions of various security forces and agencies.
- **Coordination** between central and state forces is crucial to counter Naxalism effectively.
    - The Union government plays a supportive role while state police forces take the lead.
- **Technological solutions**, like drones, should be used to minimize loss of lives of security personnel.
    - This is one of the measures for effective anti-Naxalite operations.

2) Development Initiatives:

- **The North Eastern Council (NEC)** was set up in 1972 for the socio-economic development of the North East.
    - It is a nodal agency and funds projects in agriculture, industry, health, power and tourism.
- **The Ministry of Development of North Eastern Region (MDoNER)** focuses on the development of the North East.
    - MDoNER works towards bridging infrastructural gaps in the region.
- **The "Act East" policy** seeks to connect the North East with the ASEAN region for trade and development.
- This policy aims to integrate the North East into the subcontinent's trade plans.
- **Infrastructure development** is crucial for addressing regional disparities and promoting economic growth.
    - The government is investing heavily in road, rail, and communication links in the region.
- **The North Eastern Development Finance Corporation Ltd (NEDFi)** provides financial assistance to industrial houses.
    - NEDFi supports industrial development and entrepreneurship in various sectors.
- **Capacity building** is essential for improving administration, local governance and service delivery.
    - This includes training and incentives for civil servants.
- **Regional institutions** like the North Eastern Hill University (NEHU) and North Eastern Indira Gandhi Regional Institute of Health & Medical Sciences (NEIGRIHMS) need greater attention.
    - NEHU can act as a center for excellence for regional issues, and NEIGRIHMS as a hub for tertiary health care.
- **The Integrated Action Plan (IAP)** was launched to transfer resources to Naxal-affected regions.
    - This initiative was aimed at addressing grievances in areas affected by Left Wing Extremism.
- **The Multi-Purpose National Identity Card (MNIC)** project is for registering citizens to manage illegal migration.
    - It will provide a user-friendly interface between the citizen and the government.
- **A comprehensive policy framework** is needed to promote industrialization and attract investments.
    - This can be achieved through marketing the strengths of the region and consistent capacity building.
- **Local governance institutions** such as Sixth Schedule councils and village councils are important for self-governance.
    - These institutions are designed to address the needs of tribal communities.
- **Inter-state projects** in communication, education, and health have enhanced regional cooperation.
    - The NEC has sponsored schemes that contribute to improved connectivity.

3) Political Solutions:

- **Negotiations and peace talks** are a cornerstone of the government's approach to resolving insurgencies.
    - The Mizoram Accord (1986) is a successful example of a peace accord that brought an end to decades of conflict.
- **Political empowerment** of tribal communities is a key element to address the grievances that fuel insurgencies.
    - The Sixth Schedule of the Indian Constitution provides for autonomous district councils in certain tribal areas.
- **Addressing socio-economic grievances** is crucial for achieving lasting peace.
    - The government has launched various development initiatives to tackle poverty and inequality.
- **Rehabilitation and resettlement** programs for former insurgents are important components of peace-building efforts.
    - Successful surrender and rehabilitation packages can lead to significant reductions in insurgency.
- **Involving civil society** in peace and reconciliation processes helps to broaden ownership and support for political solutions.
    - The North East Council (NEC) plays an important role in facilitating inter-state coordination and regional planning.
- **The role of the Governor** in areas governed under the Sixth Schedule of the Constitution requires examination.
    - The Governor's powers should be consistent with the intent of providing wider autonomy to the councils.
- **Addressing issues of illegal immigration** from neighboring countries is vital for strengthening the government's stance on managing the region's security.
    - Initiatives like the MNIC aim to establish a credible individual identification system and deter illegal immigration.
- **Transparency and accountability** in government functioning are essential for building trust and promoting peace.
    - Corruption in government machinery is a factor that can lead to youth joining insurgent groups.
- **Addressing the issue of dual control** for forces like the Assam Rifles.
    - There is a proposal to merge Assam Rifles with the ITBP for unified control.
- **The role of the North East Council (NEC)** requires evaluation of the balance between regional planning and inter-state coordination.
    - NEC should be an active participant in all aspects of planning for the region.

4) Constitutional Provisions:

- **The Sixth Schedule** of the Constitution grants a high degree of self-governance to tribal areas in the North East through autonomous district councils.
    - This has to some extent satisfied tribal aspirations and has prevented conflicts.
- **Article 244** of the Constitution provides for the establishment of autonomous councils to address the political aspirations of tribal groups.
    - The Bodoland Territorial Council is an example of a widely empowered council under the Sixth Schedule.
- **The 73rd Amendment** to the Constitution introduced Panchayati Raj institutions at the local level.
    - However, areas under the Sixth Schedule are exempted from the operation of the 73rd Amendment.
- **The Citizenship Act of 1955** provides a framework for determining citizenship and managing immigration.
    - The act has been amended to include provisions for registering citizens and issuing identity cards.

- **The Armed Forces Special Powers Act (AFSPA)** of 1958 empowers security forces to operate in disturbed areas.
    - The Act has been subject to controversy due to human rights concerns.
- **The Unlawful Activities (Prevention) Act (UAPA)** of 1967 is a crucial law used to counter terrorism and other unlawful activities.
    - Amendments to the UAPA have strengthened anti-terrorism laws, but it also faces opposition from human rights organizations.

Current Challenges and Way Forward

1) Economic Development Issues:

- **Infrastructure gaps** significantly hinder economic progress in the North East region, creating a need for improvements.
    - A recommendation for a **region-specific Transport Development Fund** has not yet been implemented.
- **Limited industrialization** due to weak infrastructure results in the region's economic backwardness, limiting livelihood.
    - The primary sector accounts for 55-60% of income, indicating a need to diversify the economy.
- **Unemployment** and lack of opportunities drive local youth towards insurgent groups, exacerbating instability.
    - A significant number of people from the region migrate to other cities in search of employment.
- **Lack of institutional finance** mechanisms forces people to rely on money lenders; banking systems need improvement.
    - Under-banked areas display a larger deficit of unexploited potential.
- **Inadequate formal land records** in tribal areas prevent access to loans and contribute to land disputes.
    - A credible system of land record maintenance needs to be developed.
- **The North East Industrial Policy of 1997** requires extension and suitable modifications to promote investment.
    - Tourism should be a thrust area for industrial development and job creation in the region.
- **The region has huge natural resources** (oil, gas, coal, hydro) that remain underutilized due to connectivity and infrastructure issues.
    - These resources can be harnessed for national development, reducing import dependency.
- **MSMEs are crucial** for the North East's industrial output, yet they face challenges in scaling up operations.
    - MSMEs in the region contribute to over 60% of industrial output, making their growth vital.
- **The region's proximity to Southeast Asia** presents an opportunity for trade and export, particularly for agriculture products.
    - There is a need to integrate the North East into national trade plans to fully utilize the region's potential.
- **Skill development and upgradation** are essential to enhance employability, through vocational institutes and polytechnics.
    - Export of services such as medical and health care workers and teachers could boost the economy.
- **The North Eastern Development Finance Corporation (NEDFi)** has unrealized potential, and requires a concrete action plan to develop it.
    - NEDFi was created to finance industries in the region but requires more direction.
- **Limited regional planning** has resulted in inter-state competition rather than cooperation, a hurdle to progress.
    - The North Eastern Council (NEC) should formulate a regional plan to reduce disparities.

2) Cultural Preservation Concerns:

- **The unique tribal cultures** of the North East are at risk due to modernization and external influences.
    - The region has a diverse range of ethnic groups and tribal populations.
- **Communal violence** often erupts among various tribal groups, further disrupting the socio-cultural landscape.
- Manipur has witnessed severe bouts of violence among its key communities.
- **The influx of illegal immigrants** impacts the region's demographic balance, creating social tensions and conflicts.
    - The presence of relatively more enterprising Chakma refugees has led to some unrest.
- **A lack of representation** in mainstream politics marginalizes the voices of local communities and their unique heritages.
    - The region's low representation in politics has led to the rise of insurgent groups.
- **The imposition of external norms** can erode indigenous practices, traditions, and languages if not managed well.
    - The British introduced the Inner Line Regulation meant for segregating hills from plains.
- **The customary judicial systems** require a deeper understanding and documentation for effective conflict resolution.
    - A study of the customary judicial systems is needed to understand local practices.
- **The North Eastern Hill University (NEHU)** should be developed as a center of excellence for regional issues.
    - NEHU could play a major role as a resource center for good governance and administration.
- **The North Eastern Indira Gandhi Regional Institute of Health & Medical Sciences (NEIGRIHMS)** requires strengthening.
    - NEIGRIHMS should serve as a regional hub for tertiary health care, but has not yet achieved this goal.
- **Ecotourism and green enterprises** could provide both economic opportunities and encourage conservation efforts.
    - Environmental safeguards are anticipated to be in place by 2025.
- **There is a need to strengthen** regional institutions that were vibrant but have become less effective now.
    - Regional institutions, such as the NEC, need to regain their relevance.
- **The region's biodiversity** needs preservation, including the unique flora and fauna found in its forests and national parks.
    - The Keibul Lamjao National Park is home to the brow-antlered deer, Sangai.

3) Cross-border challenges:

- The North East's **extensive international borders** with China, Myanmar, Bangladesh, and Bhutan are difficult to monitor, leading to security issues.
    - The region shares nearly 40% of India's land borders with its neighbors.
- **Insurgent groups** often find safe havens in neighboring countries, complicating counter-insurgency operations.
    - Some NSCN-IM leaders are reportedly camping in China.
- **Illegal migration** from neighboring countries strains resources and creates social tensions, affecting regional stability.
    - The settlement of Chakma refugees in Arunachal Pradesh caused some unrest.
- **Smuggling of arms and narcotics** across borders fuels insurgency and creates a "crime-insurgency nexus" in the region.
    - New narco-terrorism smuggling routes are emerging between Northeast India and Bangladesh.

- **The porous border** with Myanmar is exploited by insurgent groups for movement and training.
    - India's stance on Myanmar aids in curbing insurgency in the North East.
- **Cross-border trade** is affected by security concerns and infrastructure deficits, limiting economic benefits.
    - None of the North-Eastern states contribute significantly to India's commerce with its neighbors.
- **Cyber-attacks and misinformation** campaigns can be initiated from across borders, posing security threats.
    - Invisible warfare is conducted through non-kinetic actions like cyber-attacks.
- **External state actors** may provide support to insurgent groups, exacerbating the challenges of internal security.
    - China is seen as a potential supporter of some insurgent groups in the region.
- **The Line of Actual Control (LAC)** with China remains tense, necessitating increased vigilance and infrastructure development.
    - The ITBP plays a key role in managing the situation along the LAC.
- **The Special Frontier Force (SFF)**, a covert paramilitary unit, was raised after the 1962 China-India war.
    - The SFF is controlled by India's external intelligence agency, R&AW.
- **Dual control** over the Assam Rifles could impact border vigil, which has led to discussions on merging it with ITBP.
    - There is a proposal for a unified control of Assam Rifles under the Home Ministry.
- **The Multi Purpose National Identity Card (MNIC)** project is needed to track citizens, particularly along the border.
    - Priority should be given to areas having international borders, for implementation of the MNIC project.

4) Integration efforts:

- **The North Eastern Council (NEC)** is a nodal agency for economic and social development, but needs more focus.
    - The NEC should formulate a unified and coordinated Regional Plan, in addition to State plans.
- **The "Act East Policy"** aims to enhance connectivity and cooperation with Southeast Asia, including the North East.
    - The policy intends to promote economic cooperation, cultural ties, and strategic relationships.
- **Infrastructure projects** such as roads and railways are crucial to integrate the North East with the rest of India.
    - India plans massive infrastructure along the China border, with road and rail projects in the pipeline.
- **The Siliguri Corridor**, a narrow strip of land connecting the North East, requires strategic focus for seamless integration.
    - It is a vital part of the nation's defence architecture.
- **Cultural exchanges and people-to-people contacts** are necessary to foster a sense of national unity and identity.
    - The region has centuries-old socio-cultural ties with ASEAN countries.
- **The Sixth Schedule** of the Constitution provides a degree of self-governance to tribal areas, aiding integration.
    - The Sixth Schedule has satisfied tribal aspirations and prevented many conflicts.
- **The North Eastern Hill University (NEHU)** was set up to nurture intellectual development and can help in integration.
    - NEHU could become a center for excellence for regional issues and good governance.
- **Special incentives and facilities** are provided to officers working in the North East, but more may be needed.

    - Permitting officers to have government accommodation at their choice is a possible incentive.
- **Local officers should have more opportunities** to serve outside their states for increased professional experience.
    - More opportunities for local officers on secondment to serve outside their States is also advisable.
- **The Ministry of Development of North Eastern Region (DoNER)** was created, however, its effectiveness has been questioned.
    - The commission noted that many felt DONER compromised the efficacy of the NEC.
- **Economic integration** requires developing local entrepreneurs, skill development, and promoting investment.
    - There is a need for a major capacity building exercise for local entrepreneurs.
- **A coordinated approach** between central and state governments is necessary for effective integration and development.
    - The Union Government should have intensive interactions with the States and Union Territories while drawing up the national strategy.

Karbi Anglong Agreement:

- Signed on **November 25, 2011**, between the Central Government, Assam Government, and **UPDS** to devolve power and boost developmental activities in Karbi Anglong.
- Karbi Anglong, Assam's largest district, was listed among India's **250 most backward districts (2006)**.
- The **Karbi tribe** has long demanded a separate homeland.
- **KLNLF** has been under a Suspension of Operation (SoO) agreement since **February 11, 2010**.
- The agreement included a **Special Economic Package** for five years, above Plan funds, for the **Karbi Anglong Autonomous Territorial Council (KAATC)**.
- Part of broader efforts to address insurgency and promote regional development in the Northeast.

Mizoram: From Insurgency to Peace

- **Historical Context:** Mizoram's journey from insurgency to peace is a notable example in the Northeast. The region initially experienced unrest due to a combination of factors including:
    - **Assamese Domination:** A desire to break away from Assamese dominance was a key factor.
    - **Famine:** Unhappiness with the Assam government's relief efforts during the famine of 1959 contributed to the rise of the Mizo National Front (MNF).
    - **Language Policies**: The passage of the act in 1961 making Assamese the official language of the state was another catalyst.
    - **Secessionist Ideology:** Early insurgent groups, like the MNF, initially sought complete independence.
- **The Mizo National Front (MNF):**
    - Formed in 1961, the MNF initially aimed for independence for Mizoram.
    - The MNF established a military wing and received support from East Pakistan and China.
    - In 1966, the MNF declared independence from India, leading to a military uprising that was quickly suppressed by the Indian Army.
- **Shift Towards Autonomy:** After initial attempts at secession, Mizo leaders scaled down their demands to a separate state within the Indian Union. This shift was crucial for initiating dialogue and finding a solution. In 1973, the Mizo district of Assam was separated and given Union Territory status as Mizoram.
- **The Mizoram Peace Accord (1986):**
    - A significant turning point was the signing of an accord between the Union Government and the MNF in 1986.

    - The MNF agreed to surrender and re-enter the political process.
    - A year later, in 1987, Mizoram was granted statehood.
- **Post-Accord Peace:**
    - The accord led to a period of **complete peace and harmony in Mizoram**.
    - The state has since been recognized for its commendable implementation of development programs, and for making agriculture remunerative.
    - Mizoram is now considered one of the most peaceful states in the North East and has seen significant social and economic development.
    - The MNF is now a recognized regional political party.
- **Current Challenges**: Potential areas of conflict in Mizoram are the growing income disparities and dissatisfaction of non-Mizo district councils with the state government.
- **Hmar Insurgency**: Not all groups were satisfied with the 1986 accord and the Hmar People's Convention (HPC) was formed to seek autonomy, and later an offshoot group Hmar People's Convention Democrats (HPCD) emerged with demands for a separate tribal autonomous district.

United Liberation Front of Asom (ULFA) Movement and Its Evolution

- **Formation and Objectives:**
    - The ULFA was formed in 1979 with the aim of creating a separate state for the indigenous people of Assam.
    - It sought a return to Assam's pre-1826 status.
    - The group's initial demand was for a sovereign Assam.
- **Early Activities and Support:**
    - The ULFA gained support from Assamese youth due to factors such as unemployment, corruption, and perceived exploitation of Assam's resources.
    - They initially enjoyed considerable public support, fueled by the perception that insurgency was causing secession from Assam.
- **Decline in Popular Support:**
    - The ULFA's criminalization led to a loss of support, particularly among the urban middle classes.
    - Links with foreign agencies also contributed to their decline in public support.
    - Repeated volte-face by ULFA during negotiations with the government further eroded its credibility.
- **Government Response and Military Operations:**
    - The Indian government launched large-scale military operations, such as Operation Bajrang and Operation Rhino, to suppress the ULFA.
    - Facing continuous pressure from security forces, the ULFA relocated camps to Bhutan and Myanmar.
- **Current Status and Factions**:
    - Today, the ULFA is divided into factions.
    - One faction, led by Arabinda Rajkhowa, is engaged in talks with the government and has dropped its demand for sovereignty.
    - Another faction, led by Paresh Barua, continues to reject talks and adheres to the demand for a sovereign Assam.
- **ULFA's Continuing Activities**: The ULFA continues to make its presence felt through kidnappings, bomb blasts and selective murder of migrant workers.
- **Cross-Border Activities:** ULFA has used neighboring countries for camps and training and also has established some income generating projects in Bangladesh.
- **Links to Other Groups**: The ULFA has also been involved in joint attacks with other militant groups in the region like the NSCN-K and Bodo groups.
- **ULFA's decline**: The ULFA has lost significant power since its peak in the 1990s.

Key Differences & Lessons Learned

- **Mizoram's Success:** Mizoram's successful transition to peace is largely attributed to a comprehensive peace accord, the willingness of the MNF to join the political process, and the subsequent implementation of development programs.
- **ULFA's Complexity:** The ULFA's evolution is marked by internal divisions, shifts in objectives, and a loss of popular support due to criminalization and failed negotiations.
- **Importance of Addressing Root Causes:** Both cases highlight the importance of addressing the underlying causes of insurgency for achieving lasting peace, rather than solely relying on military solutions.
- **Role of Negotiations and Accords:** While accords are essential, their success depends on genuine dialogue, inclusivity, and full implementation.
- **Economic Development**: The case of Mizoram proves that economic development plays a huge part in the peace and development of the area, and in bringing people into mainstream society.

State Autonomy 1
State Autonomy: Constitutional Provisions 1
Legislative Relations (Articles 245-255) 1
Administrative Relations (Articles 256-263) 1
State Autonomy: Constitutional Provisions 2
Financial Relations (Articles 268-293) 2
Specific Examples of Financial Provisions in Practice 3
Evolution of Center-State Relations 3
Pre-Independence Provincial Autonomy 3
Constituent Assembly Debates 4
Debate 5
Major changes through Constitutional Amendments & Judgement 6
Case: S.R. Bommai v. Union of India (1994) 7
Background: 7
Key Issues: 7
Supreme Court's Verdict: 7
Key Rulings: 7
Jharkhand and Uttarakhand movements 7
Reorganization demands in UP and Bihar 8
State Autonomy Movements: Contemporary Dynamics 9
Regional Parties' Stance on Autonomy 9
National Parties' Approach to Centralization 10
Both State & Centre Side 10
Economic Implications of Autonomy Demands 10
Security Considerations 11
State Autonomy and Fiscal Federalism 11
1. Understanding State Autonomy 11
2. Constitutional Provisions for State Autonomy 11
3. Fiscal Federalism 11
4. Mechanisms for Fiscal Federalism 12
5. Challenges in State Autonomy and Fiscal Federalism 12
6. Recommendations for Strengthening Fiscal Federalism 12
7. Examples Highlighting the Concept 12
8. Way Forward 12
Resource Sharing Mechanisms, Development Disparities, and State-Specific Development Models 12
1. Resource Sharing Mechanisms 12
Mechanisms for Resource Sharing 13
2. Development Disparities 13
Manifestations of Disparities 13
Consequences 13
3. State-Specific Development Models 13
Key Examples 13
4. Way Forward 14
National Integrations 14

National Integration..... 15
1. National Integration: Definition and Importance..... 15
2. Unity in Diversity Principle..... 15
Mechanisms Supporting Unity in Diversity..... 16
3. Balancing Regional Aspirations..... 16
Approaches for Balancing Aspirations..... 16
4. Cross-Border Issues..... 16
Impact on Integration..... 16
Measures to Address Cross-Border Issues..... 16
5. Inter-State Disputes..... 16
Mechanisms for Resolution..... 17
6. Way Forward for National Integration..... 17

State Autonomy

State Autonomy: Constitutional Provisions

Legislative Relations (Articles 245-255)

- Parliament has exclusive power to make laws on matters not in the State or Concurrent Lists.
    - This includes the power to impose taxes not mentioned in either list.
- **Article 246** specifies that Parliament can legislate on matters in the State List when it is for the nation's interest, and the Council of States passes a resolution by a two-thirds majority.
- The executive power of every state must ensure compliance with laws made by Parliament.
    - The Union can direct a State to ensure compliance with Union laws.
- The Union can issue necessary directions to states to ensure compliance with the laws of the Parliament.

Administrative Relations (Articles 256-263)

- States' executive power should not impede Union's power, which extends to giving directions.
    - **Articles 256 and 257** ensure coordination between the Union and the States for effective Union law implementation.
    - **Article 365** provides sanctions for non-compliance, but it should be a last resort.
- The President can nominate 12 members to the Council of States based on special knowledge.
    - This includes literature, science, art, and social service.
- The President, on the advice of the Comptroller and Auditor-General of India, prescribes the form of accounts for the Union and the States.
    - Audit reports of the Union are submitted to the President.
    - Audit reports of a State are submitted to the Governor.
- The Union or a State can make grants for any public purpose.
    - This is regardless of whether they can make laws about that purpose.
- The President can direct the Governor to report on the administration of Hill Areas.
    - The Union's executive power extends to giving directions regarding these areas.
- The President can create special provisions for equitable opportunities in public employment and education for states.
    - This can vary for different parts of the State.
- The Governor can direct that a State law will not apply to an autonomous district.
    - The President can direct that a parliamentary act not apply to an autonomous region of a state.

- The Constitution provides for the creation of All India Services common to both the Union and states.
    - The President appoints and takes disciplinary action, but states can suspend officials.
- The central government determines the recruitment, training, promotion and disciplinary matters of All India Services.
- The **Inter-State Council** can investigate and advise on disputes between states and matters of common interest.
    - The President can establish an Inter-State Council to carry out these functions.
    - The Inter-State Council Order, 1990, specifies the subjects for consultation.
- The Sarkaria Commission recommended the Governor should be a non-political person appointed with the Chief Minister's concurrence.
- The Punchhi Commission emphasized 'cooperative federalism' and made over 310 recommendations.
    - This includes agreement with States before introducing legislation on the concurrent list.
    - Also included were guidelines for the appointment and dismissal of Governors and Chief Ministers.
- The 2010 report also called for limiting Union's concurrent jurisdiction to matters of national interest.
- **Article 356**, which deals with the imposition of President's rule in a state, should be used sparingly and only as a last resort.
    - This is after exhausting actions under **articles 256, 257, and 355**.
    - The invocation of **Article 356** should follow the principles of natural justice and fair consideration.
- **Article 3** allows for the formation of new states and alteration of boundaries.
    - This includes uniting a part of a state or union territory to another.
    - The President refers such matters to the concerned states for their opinion.
    - The states' opinions are not binding.

State Autonomy: Constitutional Provisions

Financial Relations (Articles 268-293)

- The **Comptroller and Auditor-General of India** certifies the net proceeds of any tax or duty, whose certificate is final.
    - Net proceeds are the proceeds of a tax or duty minus collection costs.
- The President prescribes the form of accounts for the Union and States, based on advice from the **CAG**.
    - The Union's audit reports are submitted to the President, who presents them to Parliament.
    - The State's audit reports are submitted to the Governor, who presents them to the Legislature.
- **Article 275** provides grants-in-aid to states in need of assistance, as determined by Parliament.
    - Different sums can be fixed for different states.
    - No order regarding grants is made without considering the Finance Commission's recommendations.
- **Article 282** enables the Union or a State to make grants for any public purpose.
    - This is regardless of whether they can make laws about that purpose.
- **Article 280** establishes the Finance Commission for resource transfer between the Union and states.
    - The Finance Commission makes recommendations on tax distribution and grants-in-aid.
    - It also recommends measures to augment state consolidated funds to supplement Panchayats.
- The Union or a State may make grants for any public purpose.

    - The Consolidated Fund of India and the Contingency Fund of India are regulated by law.
    - The President makes rules to regulate these funds until Parliament makes laws.
- The Constitution reflects an asymmetry between taxation powers and functional responsibilities.
    - The Centre is assigned taxes with higher revenue potential, while states have more functional responsibilities.
- The borrowing powers of the Central and State Governments are regulated by **Articles 292 and 293.**
- Mineral-rich states depend on the Centre, as the Union regulates natural resources.
    - States have limited roles in allocating their own resources.
    - States cannot directly tax minerals or capture the full economic rent from mining.
    - A Mineral Resources Rent Tax was suggested to help mineral-bearing states raise revenue.
- States bear the cost of compliance with central legislations like environmental protection laws.
    - States are not compensated for compliance costs or revenue loss.
    - The Punchhi Commission recommended compensation and including it in the Finance Commissions terms of reference.

Specific Examples of Financial Provisions in Practice

- States have demanded that the Central Government should bear at least 50% of the additional consequential burden, following the pay revision in the case of general category States and 100% of the additional burden in the case of special category State.
- Some states requested that the NDC revisit and redefine the criteria for according Special Category Status to a State.
    - This included special dispensations for less developed states.
- Some states have requested parity in funding of Centrally Sponsored Schemes.
    - For example, Uttarakhand has requested funding parity among Special Category States.
- Chhattisgarh wanted the funding pattern of all Centrally Sponsored Schemes in the IAP districts to be revisited and changed to 90:10 basis in line with North-Eastern States.

Evolution of Center-State Relations

Pre-Independence Provincial Autonomy

Add more from 1892 Onwards.

- The **Government of India Act of 1935** introduced **federal features** with a division of powers between the center and provinces.
    - The Act maintained the **supremacy of the British Parliament** while separating Burma from India.
- The Act of 1935 implemented a **system of dyarchy**, the working of which has been critically examined.
    - **Provincial autonomy** was also a key feature of this act.
- The **Simon Commission**'s recommendations were not accepted by the people of India due to not meeting national expectations.
    - Some of the commission's recommendations were adopted despite the rejection.
- **Mountbatten Plan** of June 3rd, 1947, addressed the transfer of power and the partition of India.
    - The plan led to the **Indian Independence Act of 1947**.
    - The Act ended British rule and established the Dominions of India and Pakistan.
- **Princely states** were released from obligations to the Crown by the Indian Independence Act and became technically independent.
    - They were advised to form relationships with the new dominion closest to them.

- The **Constituent Assembly** was formed to draft the Constitution of India, with representation from provinces and states.
    - The Assembly had to deal with merging princely states and integrating diverse administrative systems.
- **Disparities** existed in the constitutional relations between the Center and Provinces and Indian States during the drafting of the Constitution.
    - Indian States had the option to not accept Union or Concurrent lists.
- The **Union Powers Committee** recognized varying degrees of industrial advancement in States.
    - The committee suggested a period of transition to achieve uniformity in taxation throughout the Union.
- The Constituent Assembly had sub-committees for tribal and excluded areas to provide a scheme of administration for these areas.
    - The **Excluded and Partially Excluded Areas Sub-Committee** visited various provinces.
    - Recommendations were made for autonomous districts and councils within these areas.
    - The **North-East Frontier (Assam) Tribal and Excluded Areas Sub-Committee** made specific recommendations for the administration of these areas.
- **The States Ministry** played a role in integrating princely states into the Indian Union.
- They helped decide on the merger of some states with provinces.

Constituent Assembly Debates

- The **Constituent Assembly** served as both a constitution-making body and the legislature for the new state.
    - The assembly organized its work into five stages, including committee reports and public discussion.
- The **Congress Assembly Party** unofficially debated every provision of the Constitution before it reached the floor.
    - This party was a private forum where most of the decisions regarding the constitution were made.
- **Jawaharlal Nehru** and **Sardar Patel** were key figures in the Constituent Assembly, shaping the philosophy and provisions.
    - Nehru drafted the Objectives Resolution, while Patel focused on integrating princely states.
- **B.N. Rau**, the constitutional advisor, prepared the initial draft based on committee reports and other countries' constitutions.
- **Dr. Ambedkar** chaired the drafting committee which presented a detailed draft constitution for discussion.
- Some members of the Constituent Assembly criticized the **lack of originality** and heavy reliance on the 1935 Act and other constitutions.
    - It was noted that the constitution was largely copied from the Government of India Act and other sources.
- Concerns were raised about the **disparity in constitutional relations** between the Centre, Provinces, and Indian States.
    - Indian States were not bound to accept all subjects in the Union or Concurrent lists.
- **Maulana Hasrat Mohani** argued that the assembly was not competent because it wasn't formed after a revolution.
    - He also criticized the exclusion of the Soviet Constitution as a model.
- **Biswanath Das** raised concerns about Mayurbhanj State being treated as a separate entity within the rules.
    - He highlighted the State's impending merger with Orissa and the potential for unrest.
- **Dr. P.S. Deshmukh** highlighted the need for alignment of the rules with democratic practices in States with functioning assemblies.

    - He suggested that the speaker or president of the assembly should be the authority for filling vacancies.
- The President of the Assembly clarified that the rules were based on the recommendations of the States Ministry.
    - He also stated the rules could be altered later if changes occurred.
- The Assembly discussed the inclusion of tribal areas, with recommendations for autonomous districts and councils.
    - These districts and councils were given powers of legislation in certain areas.
    - The Central Government was to continue to administer some frontier areas, using Assam as an agent.
- The assembly discussed the need for a **Finance Commission** to address resource allocation between the center and states.
    - The Finance Commission was to recommend on tax sharing and grants-in-aid to provinces.
- The assembly considered the **division of taxes** between the center and provinces, including excise duties.
    - It was suggested that certain taxes like tobacco excise could be shared.
- The Constituent Assembly aimed to balance the need for a strong center with the aspirations for state autonomy.
    - The assembly addressed disparities in power and representation for provinces and states.

Debate

- **Arguments for a Strong Centre:**
    - One member from the United Provinces countered arguments for greater state autonomy by suggesting that those arguments echoed **"India's age-old historical tendency of disintegrating."**
    - It was argued that "only a strong centre would be in a position to think and plan for the well-being of the country as a whole". This view emphasized the importance of centralized planning and governance for national development and unity.
    - **B. R. Ambedkar** expressed his desire for a "strong united centre (hear, hear) much stronger than the centre we had created under the Government of India Act of 1935".
    - **K. M. Munshi** advocated for "a federation with a centre as strong as we can make it". These statements reflect the belief among key members of the Drafting Committee that a robust central authority was essential for stability.
    - The horrific **communal violence of 1946 and 1947** was cited as evidence for the need for a strong center. It was felt that there were "weak and vacillating executives in all the Provinces" and that a powerful, impartial central government was necessary to prevent such violence.
    - **Kazi Syed Karimuddin** emphasized the need for a "stable Government" and "a patriotic Government" with "an impartial and unbending executive, that does not bow before popular whims". This reflects a concern that decentralized power might lead to instability and a lack of uniform governance.
    - It was argued that conditions in the modern world make the **centralization of powers** inevitable, and one must consider the growth of the Federal Government in the USA.
- **Counter-Arguments and Concerns:**
    - Some members warned against the potential abuse of power by a strong center. They felt that those clamoring for seats and reservations only represented the most powerful in the community.
    - **Mahavir Tyagi** stated that reservations did not lead to real representation, but rather benefited individuals or families, and perhaps reservation should be based on class instead of caste.

    - Concerns were also raised about potential **"Hindi Imperialism,"** with one member warning that forcing people to learn Hindi would lead to the "enslavement of people who do not speak the language of the Centre".
    - A member from Orissa expressed the fear that the constitution had "so centralised power, that I am afraid, due to its very weight, the Centre is likely to break".
- **Compromise and Balance:**
    - Despite the emphasis on a strong center, there was also recognition of the importance of **state autonomy** and **decentralization**. The constitution was intended to balance the demands of diversity with the needs of unity.
    - The framers of the Constitution kept in view the difference between **decentralization** and **disintegration**, and between **unity** and **centralization**. They sought to create a system that could integrate diverse regions while ensuring a strong central authority.

Major changes through Constitutional Amendments & Judgement

- Indian Constitution is neither purely federal nor purely unitary, ensuring state autonomy in their allocated spheres.
    - Constitutional distribution of powers exists in legislative, executive and administrative fields.
- The accounts of the Union and States are kept as the President prescribes, with advice from the Comptroller and Auditor-General.
    - Audit reports of Union submitted to the President; state reports to the Governor.
- Finance Commission makes recommendations for distribution of tax proceeds between Union and States.
    - Also suggests principles for grants-in-aid and augmenting State Consolidated Funds.
- All India Services are common to both Union and States; appointments and discipline is with President.
    - These services are meant to bring cooperation in administration.
- Pressure groups influence administration to promote or protect their interests.
    - They act as a stabilizing mechanism but may also create pressure on the system.
- Administrative personnel is divided into generalists and specialists based on their functions.
    - Generalists are in the Indian Administrative Service (IAS), specialists in other central services.
- Generalist civil service was founded when specialized knowledge was not required in administration.
- Specialists feel that generalists do not have specialized knowledge for policy making.
- Administrative Reforms Commission (ARC) suggested a method for manning policy level posts.
    - Examination for officers with 8-12 years of experience, and allotment to a specialty.
- The Sarkaria Commission and the National Commission to Review the Working of the Constitution (NCRWC) influenced the Punchhi Commission.
    - The Punchhi Commission emphasized cooperative federalism and made over 310 recommendations.
- Basic structure of the Constitution cannot be altered; includes federal structure.
    - Also includes supremacy of the Constitution, republican form, secular character, separation of powers.
- Several constitutional amendments have been made that impact centre-state relations.
    - Amendments include changes to the First Schedule and modifications to the powers of the Governor.
- The Constitution has been amended to provide a third tier of government at the local level.
    - This creates a three-tier arrangement for sharing power and responsibilities.
- The space for state autonomy has expanded and constricted in specific areas.
    - Variations exist in how states experience the federal framework.

- States have demanded compensation for the costs of complying with central legislation.
    - They have also demanded a greater share of tax revenues and opposed centralizing principles.
- Some states have demanded a revisit of criteria for special category status.
    - They have argued for a 90:10 funding pattern for centrally sponsored schemes.
- The Finance Commission can make recommendations for revenue assignment to the Provinces.
    - The commission has the power to suggest changes in the heads of revenue assigned to the provinces.
- The Constituent Assembly debated the need for a strong centre versus provincial autonomy.
    - Some members felt the center was too strong, while others advocated for a very strong center
- There have been differing views on the nature of Indian federalism, with some viewing it as unitary
    - Some members wanted more democratic decision making with greater state autonomy and input
- Tribal areas were recognized as needing special administrative treatment.
    - Sub-committees recommended the formation of autonomous districts within states.
- The Central government was to continue to administer frontier tracts with Assam as its agent.
    - The central government had the ability to integrate these areas into provincial administration.
- There was debate about whether the Constituent Assembly was a competent body, given the lack of revolution.
    - Also debated was the copying of other nations' constitutions, and why the Soviet Union model was not followed.

Case: S.R. Bommai v. Union of India (1994)

Background:

- The case arose from the dismissal of multiple state governments under **Article 356** (President's Rule).
- It questioned whether the Centre had misused its powers to dismiss democratically elected state governments.
- The main issue was whether judicial review could examine the proclamation of President's Rule.

Key Issues:

1. **Extent of judicial review under Article 356**.
2. **Limits on the Centre's power to impose President's Rule in states**.
3. **Nature of federalism under the Indian Constitution**.

Supreme Court's Verdict:

Key Rulings:

1. **Judicial Review**:
    - Proclamations under Article 356 are subject to judicial review.
    - Courts can strike down arbitrary or mala fide impositions of President's Rule.
2. **Test of Majority**:
    - The majority of a state government should be tested only on the floor of the Legislative Assembly and not decided by the Governor or the Centre.
3. **Federal Structure**:
    - Indian federalism is not rigid but a cooperative one.
    - States are not mere appendages of the Centre, and their autonomy should be respected.
4. **Accountability**:

    - If the Centre dissolves a state assembly under President's Rule, the dissolved assembly cannot be revived after judicial review.

Jharkhand and Uttarakhand movements

- **Jharkhand's demand for statehood** stemmed from the **marginalization of tribal populations** and their unique cultural identity.
    - The movement sought to address issues of **land alienation, resource exploitation, and lack of development**.
- The **Chota Nagpur region**, with a high tribal population, was central to the Jharkhand movement.
    - **Tribal communities** in this region felt that their interests were not adequately represented.
- The **demand for a separate state** was also fueled by economic disparities and the **neglect of tribal areas** by the Bihar government.
    - The region had a history of **social and political movements** that predated the statehood demand.
- The **Santhal Parganas** and other areas with significant tribal populations were key areas of the movement.
    - These regions experienced **exploitation by outsiders**, intensifying calls for self-governance.
- The **Tribes Advisory Council** was seen as a mechanism to safeguard tribal rights and interests.
    - This Council was viewed as essential for protecting **land rights, cultural practices, and economic interests**.
- The creation of Jharkhand as a separate state was achieved through a political process after long agitation.
    - The movement highlighted the need for **specific administrative and legal frameworks** to protect tribal communities.
- **Uttarakhand's statehood demand** was driven by a combination of factors including geographical isolation and neglect.
    - The movement focused on the **underdevelopment of the hill region** and a need for local governance.
- **Geographical and cultural distinctiveness** contributed to the demand for a separate state from Uttar Pradesh.
    - The region's **unique topography and ecological importance** were key factors.
- The demand also involved a desire for better control over the state's resources, especially minerals.
    - The state felt a need to **address local environmental and developmental concerns**.
- The movement gained momentum due to the **lack of infrastructure, employment opportunities, and social services**.
    - The state had significant deficits in human development which spurred the movement.
- **Uttarakhand** also argued for parity in funding of centrally sponsored schemes among the Special Category States.
    - They were being denied the 90:10 funding pattern in several centrally sponsored schemes.
- The issue of compensation for states was raised by the Punchhi Commission and the 13th Finance Commission.
    - States demanded compensation for the cost of compliance with central legislation.
- Both movements highlighted the need for **recognition of regional disparities and aspirations** within the Indian Union.
    - These movements have influenced the broader discourse on state autonomy and federalism.

Reorganization demands in UP and Bihar

- **Reorganization demands in UP and Bihar** arose from **regional disparities** and a desire for better governance.
    - These movements sought to address **economic imbalances** and social neglect within larger states.
- **Historical context:** UP and Bihar were large states with diverse regions and differing needs.
    - This led to **calls for smaller, more manageable administrative units** to improve efficiency
- **Main demands** in UP focused on the creation of **Uttarakhand**, which was eventually granted statehood.
    - **Uttarakhand** sought autonomy due to its unique geographical and cultural identity
- **Economic factors** played a major role in the demands, with regions feeling neglected and exploited.
    - The movements highlighted issues of **resource distribution, lack of development, and unemployment**
- **Social dimensions** included **caste and tribal issues**, with marginalized groups seeking greater representation.
    - These groups felt their interests were not being addressed within larger state structures.
- **Resolution/current status** for UP includes the creation of **Uttarakhand** as a separate state.
    - This led to improved focus on regional development and governance in the newly formed state.
- **Bihar** saw demands for the creation of **Jharkhand**, which was eventually granted statehood.
    - The **Jharkhand movement** was driven by the marginalization of tribal populations and resource exploitation
- **Economic factors** in Bihar included the need for **better management of mineral resources** in the Chota Nagpur region.
    - The state was not able to adequately address the needs of tribal communities.
- **Social dimensions** in Bihar involved the **protection of tribal land and cultural rights** from outside influence.
    - The **Tribes Advisory Council** was a focus for such protections
- **Resolution/current status** for Bihar resulted in the formation of **Jharkhand** as a separate state.
    - This facilitated **focused administration and development efforts** in the tribal areas.
- Both UP and Bihar had regions with a **history of social and political movements** predating the reorganization demands.
    - These movements **mobilized public opinion** and created a push for the formation of new states.
- **The reorganization of UP and Bihar** resulted in more manageable administrative units.
    - These changes also addressed some, but not all, **longstanding grievances**.
- The creation of new states in UP and Bihar was influenced by recommendations of various commissions.
    - These commissions highlighted the need for **regional balance and inclusive development**.
- The movements highlighted the need for **greater state autonomy and regional self-determination** within the Indian Union.
    - These demands also reflected underlying issues of **inequality, neglect, and the desire for local governance**

State Autonomy Movements: Contemporary Dynamics

Regional Parties' Stance on Autonomy

- Advocate greater fiscal autonomy for states to meet regional aspirations effectively.
  - Demand more share in central taxes (N.K. Singh FRBM Report).
- Emphasize cultural and linguistic autonomy to preserve unique identities.
  - Tamil Nadu's resistance to Hindi imposition (National Education Policy debates).
- Oppose central schemes overriding state policies, citing federal imbalance.
  - Resistance to GST compensation delays (RBI State Finances Report).
- Highlight grievances over resource allocation favoring central projects.
  - Focus on coal royalties in mineral-rich states ([NITI Aayog Report 2020]).
- Advocate against excessive central interference in law and order matters.
  - Example: West Bengal's opposition to BSF jurisdiction extension ([MHA Notifications]).
- Demand devolution of powers in subjects under Concurrent List.
  - Example: Health and Education policy disputes ([Second ARC Recommendations]).

National Parties' Approach to Centralization

- Stress strong central control for uniformity in national policy implementation.
  - Cites GST rollout as a unifying tax reform ([Finance Commission Report]).
- Advocate central schemes for socio-economic development across all states equally.
  - Examples: PM-Kisan, Ayushman Bharat ([NITI Aayog Reports]).
- Highlight central oversight in national security to maintain internal stability.
  - Example: AFSPA extensions in disturbed areas ([Supreme Court Verdicts]).
- Prioritize cooperative federalism while ensuring a strong central framework.
  - Example: NITI Aayog replacing Planning Commission ([2015 NITI Aayog Paper]).
- Use financial aid as a tool to align states with national priorities.
  - Performance-based grants for rural development ([14th Finance Commission]).
- Advocate uniform educational and labor reforms to enhance competitiveness.
  - Example: National Education Policy focus on central guidelines ([NEP 2020]).

Both State & Centre Side

- **Regional parties** advocate for greater state autonomy and increased financial resources.
  - They seek more control over mineral resources and direct taxation powers.
- Mineral-rich states want a say in mineral concessions and to benefit their people.
  - Odisha proposed a Mineral Resources Rent Tax at 50% of surplus.
- States face financial burdens due to central laws, without compensation.
  - Compliance costs for environmental, wildlife, and forest acts borne by states.
- **The Punchhi Commission** also highlighted the issue of compensation for states.
  - Recommended a mechanism to institutionalize compensation for additional expenditures by states.
- States demand that the central government bear additional burdens.
  - They seek at least 50% burden sharing for general category states, 100% for special states.
- Some states have requested revisiting of criteria for Special Category Status.
  - Odisha and Uttarakhand seek special dispensations.
- **The Indian Constitution** distributes powers between the Union and the States.
  - This division is in the legislative, executive, and administrative fields.
- States are granted autonomy in their designated areas under the Constitution.
  - They should have the freedom to act in state and concurrent fields.
- The Union has the authority to give directions to states when necessary.
- Articles 256, 257, and 365 aim to secure coordination between the Union and states.
- **The Sarkaria Commission** emphasized the importance of cooperative federalism.
  - This is crucial for maintaining India's unity, integrity, and development.

- **The Punchhi Commission** made recommendations for better centre-state relations.
    - These recommendations include agreements before legislation on concurrent subjects.
- **The Punchhi Commission** also suggested a fixed tenure for Governors with guidelines for appointments.
    - Clear guidelines for the dismissal of Chief Ministers were also proposed.

Economic Implications of Autonomy Demands

- Fiscal strain on the Centre due to increased devolution of financial resources to states.
    - Example: GST compensation disputes and delayed payments ([CAG Reports 2021]).
- Regional economic policies may create competition among states, impacting national coherence.
    - Example: Tamil Nadu's separate industrial policies ([State Budget 2023-24]).
- Autonomy demands can reduce efficiency of centrally funded schemes in states.
    - Example: Opposition to central guidelines in MGNREGA ([Rural Development Ministry Reports]).
- Regional protectionism may lead to unequal development across states, widening disparities.
    - Example: Preferential employment for locals in Maharashtra ([Labour Law Review 2022]).
- Loss of economies of scale in centralized policies if states adopt divergent frameworks.
    - Example: State-specific labor codes vs. national labor reforms ([Second ARC Recommendations]).
- Hindered foreign investment due to fragmented economic policies across states.
    - Example: Investors' concerns over Andhra Pradesh's bifurcation policies ([World Bank Ease of Doing Business Report]).

Security Considerations

- Autonomy demands may fuel separatist tendencies, risking national integrity.
    - Example: Khalistan movement linked to demands for Punjab's autonomy ([Intelligence Bureau Reports]).
- Increased state control over law enforcement could weaken central response to insurgencies.
    - Example: State-Centre clash over deployment of paramilitary forces in Kashmir ([MHA Reports 2020]).
- Autonomy may complicate intelligence sharing between Centre and states, delaying response.
    - Example: 26/11 Mumbai attacks exposed coordination failures ([Ram Pradhan Committee Report]).
- Proliferation of regional militias under weak central oversight in high-conflict areas.
    - Example: Nagaland's armed groups negotiating separate frameworks ([NSCN Peace Accord 2015]).
- Border state autonomy may lead to policy conflicts in countering cross-border infiltration.
    - Example: West Bengal's opposition to BSF jurisdiction increase ([Home Ministry Notifications]).
- Security infrastructure disparities among states may leave gaps in internal defense.
    - Example: Northeast states' weaker policing frameworks ([BPRD Report 2021]).

State Autonomy and Fiscal Federalism

---

1. Understanding State Autonomy

- **Definition**: The degree to which states have the power to govern themselves independently within a federal structure.

- **Importance**: Ensures decentralization, addressing regional diversity, and empowering local governance.

2. Constitutional Provisions for State Autonomy

- **Seventh Schedule**: Division of powers among Union, State, and Concurrent lists.
  - **Union List (97 items)**: Defense, foreign affairs.
  - **State List (66 items)**: Police, agriculture, public health.
  - **Concurrent List (52 items)**: Education, forest, marriage laws.
- **Article 246**: Legislative jurisdiction based on the lists.
- **Article 356**: Imposition of President's Rule, limiting autonomy during emergencies.

---

3. Fiscal Federalism

- **Definition**: The financial relations between the central government and state governments in a federal structure.
- **Objective**: Ensure states have sufficient resources to perform their functions effectively.

---

4. Mechanisms for Fiscal Federalism

1. **Finance Commission (Article 280)**:
   - Determines distribution of tax revenue between the center and states.
   - Example: 15th Finance Commission (2021-26) recommended 41% devolution of central taxes to states.
2. **Goods and Services Tax (GST)**:
   - Unified tax structure but led to states losing fiscal autonomy.
   - **GST Compensation**: Ensures revenue protection for states post-GST implementation.
3. **Grants-in-Aid (Article 275)**:
   - Provided by the center to states for specific schemes or needs.
4. **Borrowing Limits (Article 293)**:
   - States require central approval for external borrowing beyond limits.

---

5. Challenges in State Autonomy and Fiscal Federalism

1. **Vertical Imbalance**:
   - Center collects most taxes, but states bear expenditure responsibilities.
   - Example: Center's share in taxes is 62%, while states handle 60% of developmental spending.
2. **Horizontal Imbalance**:
   - Resource-rich states vs. resource-poor states.
   - Example: Tamil Nadu vs. Bihar in per capita revenue generation.
3. **Over-Centralization**:
   - Centrally sponsored schemes with rigid guidelines dilute state autonomy.
4. **GST Challenges**:
   - Delay in compensation payments affects states' finances.

---

6. Recommendations for Strengthening Fiscal Federalism

1. **Second ARC Recommendations**:
   - Greater flexibility in resource use by states.
2. **Finance Commission Suggestions**:
   - Incentivize states based on performance (e.g., ease of doing business, education).
3. **Greater Decentralization**:
   - Devolution of funds and functions to local governments.

---

7. Examples Highlighting the Concept

1. **Kerala's Fiscal Autonomy**:
   - Innovative tax reforms for revenue generation, e.g., Social Security Cess.
2. **Bihar's Dependency on Center**:
   - High reliance on central grants due to limited own-tax revenue.

3. **GST Dispute**:
    - Punjab and West Bengal raised concerns about delays in GST compensation.

---

8. Way Forward
- Ensure timely GST compensation and enhance tax autonomy for states.
- Promote cooperative federalism through collaborative fiscal planning.
- Adopt technology for transparent fund allocation and utilization.

Resource Sharing Mechanisms, Development Disparities, and State-Specific Development Models

---

1. Resource Sharing Mechanisms
- **Definition**: Allocation of resources (financial, natural, human) between the central and state governments to ensure equitable growth.
- **Importance**: Supports decentralization and addresses resource-related conflicts among states.

Mechanisms for Resource Sharing
1. **Finance Commission (Article 280)**:
    - Determines vertical (center-state) and horizontal (among states) distribution of tax revenues.
    - Example: 15th Finance Commission allocated 41% of central taxes to states.
2. **Goods and Services Tax (GST)**:
    - Single tax system; revenue shared among center and states.
    - GST Council: Joint decision-making on tax rates and slabs.
3. **Natural Resource Allocation**:
    - **Coal, oil, and minerals**: Royalty payments shared with resource-rich states.
    - Example: Coal mining royalties in Jharkhand and Odisha.
4. **Centrally Sponsored Schemes (CSS)**:
    - Fund-sharing between center and states for development programs.
    - Example: MGNREGA (75:25 funding ratio for non-Himalayan states).
5. **Borrowing and Grants**:
    - Center provides conditional grants or approves loans.
    - Example: Special grants to northeastern states under Article 275.

---

2. Development Disparities
- **Definition**: Uneven distribution of economic growth and access to resources among regions, leading to socio-economic gaps.
- **Factors Leading to Disparities**:
    - **Historical**: Colonial policies favoring certain regions (e.g., Bengal Presidency).
    - **Geographic**: Resource availability varies (e.g., coastal vs. landlocked states).
    - **Policy Bias**: Infrastructure and industrial projects concentrated in specific areas.

Manifestations of Disparities
1. **Per Capita Income Gap**:
    - Punjab and Haryana: High-income states.
    - Bihar and UP: Low per capita income.
2. **Infrastructure Imbalance**:
    - Example: Southern states have better healthcare and education facilities compared to northern states.
3. **Urban-Rural Divide**:
    - Urban areas like Bengaluru and Mumbai grow rapidly, while rural areas lag.
4. **Sectoral Contribution**:
    - Example: Agriculture-dependent states like MP vs. industrial hubs like Gujarat.

Consequences

1. Migration from underdeveloped states to developed regions.
2. Rising unemployment and poverty in backward regions.
3. Regionalism and political instability (e.g., demand for separate states).

---

3. State-Specific Development Models

- **Definition**: Tailored approaches adopted by states to address their unique socio-economic and geographical challenges.

Key Examples

1. **Kerala's Human Development Model**:
    - Focus: Health, education, and social welfare.
    - Result: High HDI, literacy rate (96.2%).
    - Example: Kudumbashree Mission for women empowerment.
2. **Gujarat's Industrial Growth Model**:
    - Focus: Manufacturing, ports, and infrastructure.
    - Result: High FDI inflows and industrial output.
    - Example: Dholera Smart City project.
3. **Punjab's Agriculture-Based Model**:
    - Focus: Green Revolution technologies for high-yield crops.
    - Result: Surplus in food grain production but ecological challenges like soil degradation.
4. **Odisha's Mineral-Based Development**:
    - Focus: Leveraging mineral resources for industrial growth.
    - Result: Growth in steel and mining sectors but social unrest in tribal areas.
5. **Rajasthan's Water Conservation Model**:
    - Focus: Traditional techniques (e.g., johads) and modern irrigation.
    - Example: Mukhya Mantri Jal Swavlamban Abhiyan.

---

4. Way Forward

1. **Balanced Resource Allocation**:
    - Strengthen Finance Commission's equitable sharing formula.
2. **Policy Innovation**:
    - Adopt state-specific models for addressing disparities.
3. **Cooperative Federalism**:
    - Ensure states and center work collaboratively on developmental issues.
4. **Technology-Driven Solutions**:
    - Example: GIS mapping for resource allocation and tracking.
5. **People-Centric Policies**:
    - Focus on grassroots development with local governance involvement.

National Integrations

- The Indian Constitution is neither purely federal nor purely unitary, with a clear distribution of power between the Union and states.
    - States should have autonomy in their designated areas of activity.
- **Cooperative federalism** is essential for India's unity, integrity, and development.
    - The Punchhi Commission emphasized this concept.
- **Strong states are fundamental to a strong nation**.
    - NITI Aayog's State Support Mission aims to engage with states for transformational objectives.
- The All-India Services (IAS, IPS, IFS) are a key mechanism for **centre-state cooperation**.
    - Members occupy key positions in both the central and state governments.
    - The central government handles recruitment and disciplinary matters, but states have immediate control.

- **Regional disparities** need to be addressed, with special support for areas like the North-East and Himalayas.
    - NITI Aayog has taken special steps for these regions.
- The National Education Policy requires collective action by the Centre and states for implementation.
    - All stakeholders should develop a clear roadmap for the National Education Policy.
- The national Multi-dimensional Poverty Index (MPI) helps measure and address factors hindering growth.
    - The MPI provides data for states, union territories, and districts to highlight regional disparities.
- States should focus on promoting trade, tourism, and technology (3Ts) with the assistance of Indian missions.
    - States should aim to reduce imports and increase exports.
- Increased GST collection requires collective action between the Centre and states.
    - This is crucial for strengthening the economic position of the country.
- The Sarkaria Commission and the National Commission to Review the Working of the Constitution (NCRWC) provided input for the Punchhi Commission.
- The Administrative Reforms Commission (ARC) recommended a system for higher policy positions that tests for broad conceptual and managerial skills.
    - This system would include an examination open to all higher service officers with 8–12 years of experience.
- The ARC also proposed eight specialities for officers based on their aptitude and background: personnel and manpower, economic, financial, agricultural, industrial, social and educational, internal security and defence and general administration.
- The Centre should assist states with liabilities from area-specific schemes.
    - Special assistance is given to states, considering socio-economic and geographical factors.
- State factsheets are developed to track state performance in various sectors and provide evidence-based inputs for policy making.
- NITI Aayog and UNDP have jointly produced a compendium of best practices in the social sector.
- Pressure groups try to influence administrative and political systems to promote their interests.
    - These groups are important in the administrative system.
- The Constitution provides for the creation of additional All-India Services common to the Union and states.
    - The recruitment, training and promotion of these services is determined by the central government.
- The Centre has the authority to levy a surcharge when conditions require it.
    - Such occasions should be rare.
- The Central government should be able to require state governments to implement schemes for scheduled areas.
- The central government should also create a commission to examine the progress of scheduled areas and the tribes after a period of ten years.
- States are not presently compensated for compliance costs for central legislation like the Environment Protection Act.
    - The Punchhi Commission raised the issue of compensation for states.
- A Finance Commission should be appointed to deal with points of conflict between the centre and the units.
    - The Finance Commission members are to be appointed by the President.
- The Constituent Assembly acknowledged that, with regard to states, the situation was in constant flux and changes to the rules were necessary and expected.

National Integration

---

1. National Integration: Definition and Importance

- **Definition**: The process of bringing together diverse cultural, linguistic, religious, and regional groups into a unified and cohesive nation.
- **Importance**:
    - Promotes harmony and reduces regionalism.
    - Strengthens democracy and socio-economic stability.
    - Ensures equitable development and national security.

---

2. Unity in Diversity Principle

- **Definition**: Acknowledging and respecting cultural, linguistic, and religious diversity while maintaining a collective national identity.
- **Significance**:
    - Reflects India's pluralistic society as enshrined in the Constitution (Preamble, Fundamental Rights).
    - Celebrates festivals like Diwali, Eid, Christmas as symbols of unity.

Mechanisms Supporting Unity in Diversity

1. **Constitutional Provisions**:
    - **Article 29**: Protection of cultural and educational rights of minorities.
    - **Article 51A(e)**: Duty to promote harmony among diverse groups.
2. **Institutions and Policies**:
    - National Integration Council (NIC): Promotes communal harmony.
    - Reservation Policies: Address historical inequalities.
3. **Examples**:
    - Linguistic diversity with 22 official languages (Eighth Schedule).
    - Inter-faith initiatives like Sarva Dharma Samabhava.

---

3. Balancing Regional Aspirations

- **Challenges**:
    - Uneven development and identity politics (e.g., Gorkhaland, Telangana).
    - Autonomy demands in regions like Kashmir and the Northeast.

Approaches for Balancing Aspirations

1. **Decentralization**:
    - Strengthening local governance via Panchayati Raj and urban bodies.
    - Example: Sixth Schedule provisions for autonomous councils in the Northeast.
2. **Special Provisions for States**:
    - **Article 371**: Ensures development and cultural autonomy in states like Nagaland, Maharashtra.
3. **Equitable Development**:
    - Focused investment in backward regions through schemes like Aspirational Districts Programme.
4. **Cooperative Federalism**:
    - Example: NITI Aayog's role in fostering collaboration among states.

---

4. Cross-Border Issues

- **Definition**: Challenges arising from geographical proximity and shared borders with neighboring nations.
- **Major Issues**:
    - Infiltration and illegal migration (e.g., Rohingya crisis, Bangladesh border).
    - Cross-border terrorism (e.g., Pakistan-sponsored terrorism in Jammu & Kashmir).
    - Smuggling and trafficking of goods, arms, and narcotics.
    - Boundary disputes (e.g., Kalapani with Nepal, Arunachal Pradesh with China).

Impact on Integration

- Fuels regional instability, ethnic conflicts, and communal tensions.
- Example: NRC and CAA debates leading to societal polarization.

Measures to Address Cross-Border Issues

1. **Bilateral Agreements**:
    - Example: Land Boundary Agreement (2015) with Bangladesh.
2. **Border Security and Infrastructure**:
    - Deployment of BSF and building border fences.
    - Example: Integrated Check Posts (ICPs) for regulated movement.
3. **Diplomacy and Confidence-Building**:
    - Example: Kartarpur Corridor for India-Pakistan religious harmony.

---

5. Inter-State Disputes

- **Definition**: Conflicts between states over resources, boundaries, or governance.
- **Key Examples**:
    - **Water Disputes**: Cauvery river dispute (Karnataka-Tamil Nadu).
    - **Boundary Disputes**: Assam-Mizoram clashes.
    - **Resource Sharing**: Power-sharing disputes over hydropower projects.

Mechanisms for Resolution

1. **Legal Framework**:
    - Interstate River Water Disputes Act, 1956.
    - Supreme Court as the adjudicator under Article 131.
2. **Institutions**:
    - Interstate Councils under Article 263.
    - Tribunals like the Krishna Water Disputes Tribunal.
3. **Cooperative Federalism**:
    - Example: NITI Aayog facilitating dialogue among states.

---

6. Way Forward for National Integration

1. **Strengthen Constitutional Safeguards**:
    - Protect regional identities while fostering national identity.
2. **Promote Inter-Cultural Exchanges**:
    - Programs like Ek Bharat Shreshtha Bharat.
3. **Equitable Development**:
    - Reduce disparities through targeted policies for backward regions.
4. **Inclusive Governance**:
    - Representation of diverse groups in decision-making.
5. **Peaceful Resolution of Conflicts**:
    - Institutional mechanisms for resolving inter-state and cross-border disputes.

National Integration 1
Definition and significance in Indian context 1
Historical Evolution of National Integration in Post-Independence India 1
1. Challenges in the Early Post-Independence Period 1
2. Adoption of the Constitution (1950) 2
3. Linguistic Reorganization of States (1956) 2
4. Communal Harmony and Secularism 2
5. National Integration Council (1961) 2
6. Green Revolution and Economic Integration (1960s–70s) 2
7. Regional Movements and Insurgencies (1970s–80s) 2
8. Post-Liberalization Era (1991 Onwards) 2
9. Contemporary Efforts for National Integration 2
Way Forward 2
Core Problems of National Integration: 3
Socio-cultural challenges 3
Political-Administrative Challenges 3
Economic challenges 4
National Integration Council (NIC) 5
Hooda Committee Suggestions for a Draft National Security Strategy (NSS) 6
Kargil Review Committee (KRC): 6
Madhukar Gupta Committee 6
National Integration: Solutions and Way Forward 7
● Policy Measures 7
● Social Reforms 8
● Economic Initiatives 8
● Administrative Steps 9
● Role of Civil Society 9
National Integration Scheme 10

National Integration

Definition and significance in Indian context

- **National integration** is the awareness of a **common identity** among citizens of a country.
    - It strives to unite disparate groups into a single nation.
- It is critical in India to enhance harmony among all parts of society.
- **National security** is a function of a country's external environment and internal situation.
    - Lack of focus can lead to issues like terrorism, extremism, and cyber threats.
- India was a geographical entity divided into princely states in ancient times.
    - British rule united India administratively but did not create national unity.
- **Communalism** is a disturbing problem and a threat to national integration.
    - British rulers used communal division as a tool to divide Indians.
- The Indian constitution declares India a **secular state**.
    - The word 'secular' was added to the Preamble in 1976.
- India has a complex diversity that leads to ethnic clashes.
- This creates a fractured society where insurgents can easily penetrate.
- **Regionalism** is a problem in India due to different traditions, languages and cultures.
    - It can cause disintegration and disputes between regions.

- **Casteism** is a concept in India that has segregated society and damages national unity.
    - It causes feelings of inequality and injustice among the oppressed.
- **Multilingualism** is a feature of India that can cause strife and violence.
    - People compete with others who speak another language.
- **Article 244** of the Indian Constitution relates to the administration of scheduled areas.
    - It provides for autonomous councils with financial and legislative powers.
- The **Panchayat Extension to Scheduled Areas Act, 1996** (PESA) aims to empower people to exercise control over their own resources.
    - It is intended to address problems of exploitation and self-governance.
- **The Forest Rights Act for Scheduled Tribes** gives rights to forest dwellers and pre-existing rights.
    - It helps address the tension between land and related concerns.
- The **National Integration Council (NIC)** was established in 1961.
    - Its aim is to investigate and give recommendations to deal with national integration.
- The **Bezbaruah Committee** in 2013 recommended increased representation in the central government and nodal police stations for people from North East.
- **National integration** means creating a mental outlook that inspires loyalty to country above narrow interests.
- **Radicalization** is a threat that has spread in India, especially in areas with religious and ethnic conflicts.
    - It is also causing violence in the form of mobs, riots and other disruptions.
- **Terrorism** is a threat to international stability motivated by fundamentalist ideologies.
    - It is backed by secret financial networks.
- **Cybersecurity** challenges are threats to internal security.
- The government has created a vast system to address internal security concerns.

Historical Evolution of National Integration in Post-Independence India

1. Challenges in the Early Post-Independence Period

- **Partition (1947)**: Communal violence during the partition resulted in social and cultural fragmentation.
    - **Data/Fact**: Over 1 million lives lost; 15 million displaced.
    - **Example**: Refugee rehabilitation programs under the Nehru government.
- **Princely States**: Integration of 562 princely states into the Indian Union.
    - **Key Measure**: Instrument of Accession.
    - **Example**: Sardar Patel's efforts and Hyderabad Operation Polo (1948).

2. Adoption of the Constitution (1950)

- **Unity in Diversity**: Federal structure with unitary bias for national cohesion.
    - **Key Provisions**: Fundamental Rights (Article 14, 19, 25) and DPSPs promoting equality.
    - **Example**: Article 15 prohibits discrimination on grounds of religion, caste, gender.

3. Linguistic Reorganization of States (1956)

- **Demand for Linguistic States**: Led to formation of Andhra Pradesh (1953), followed by States Reorganization Act.
    - **Key Debate**: Balancing regional identities with national unity.
    - **Example**: Formation of Maharashtra and Gujarat (1960).

4. Communal Harmony and Secularism

- **Emphasis on Secular Values**: Separation of religion and state under Nehruvian vision.
    - **Policy**: Neutrality toward all religions.
    - **Example**: Ban on communal organizations like the RSS post-Gandhi assassination.

5. National Integration Council (1961)

- **Objective**: Counter communalism, regionalism, and casteism.
    - **Initiative**: Periodic meetings of political leaders and civil society.
    - **Example**: Resolution against communal violence after 1969 Gujarat riots.

6. Green Revolution and Economic Integration (1960s–70s)
- **Economic Cohesion**: Reduced inter-regional disparities through agricultural reforms.
    - **Outcome**: Increased food security and reduced dependence on imports.
    - **Example**: Punjab and Haryana as models of success.

7. Regional Movements and Insurgencies (1970s–80s)
- **Regional Aspirations**: Addressing demands for autonomy in North-East, Punjab, and Tamil Nadu.
    - **Key Acts**: Creation of Nagaland (1963), Mizoram Accord (1986).
    - **Example**: Rajiv Gandhi's Assam Accord (1985) to address Assam agitation.

8. Post-Liberalization Era (1991 Onwards)
- **Economic Globalization**: Promoting inter-state and international cooperation.
    - **Key Program**: Infrastructure projects like Golden Quadrilateral for connectivity.
    - **Example**: Enhanced trade between states reducing regional economic gaps.

9. Contemporary Efforts for National Integration
- **Educational and Cultural Policies**: NCERT textbooks promote national unity.
    - **Programs**: 'Ek Bharat, Shreshtha Bharat' (2015).
    - **Example**: Cultural exchanges between Maharashtra and Odisha.
- **Legislation**: Prevention of Insults to National Honour Act (1971).
    - **Example**: Strict action against disrespect to the national flag or anthem.

Way Forward
- Strengthening **inclusive policies** through federal and grassroots participation.
- Promoting **regional development** to address disparities and avoid alienation.
- Implementing **awareness campaigns** on communal harmony and diversity.

Core Problems of National Integration:
Socio-cultural challenges
- **Religious diversity**, while a strength, is also a challenge to national integration.
    - **Communalism** remains a significant threat, causing social unrest and violence.
    - Political manipulation of religion leads to communal riots and distrust.
    - Sectarian strife between Shia and Sunni is a cause for concern.
- **Linguistic differences** and the presence of many languages can cause division.
    - India has approximately 2000 languages and dialects, creating potential for conflict.
    - Imposing a single official language has been contentious, especially for non-Hindi speakers.
    - **Multilingualism** is a feature of India, but can also be a cause of strife.
    - Linguistic barriers can also create war and conflict.
- **Regionalism** is also a threat to national integration.
    - It is linked to the desire for sub-regional autonomy and can lead to conflict between states.
    - Regional disparities in development can also cause resentment.
- **Caste divisions** and social inequalities hinder national unity and integration.
    - **Casteism** creates a lack of social harmony and perpetuates discrimination.
    - The oppression of upper castes damages the feeling of solidarity.

- **Social inequalities** contribute to a fractured society and make it easier for insurgents to penetrate.
- The perception of being neglected can increase the chances of youth joining insurgents.
- Racial bias against people from the North-East contributes to a sense of alienation.
- **Alienation** from conventional political processes leads to some groups boycotting dialogue and elections.
- Gaps between India and its Northeast lead to a sense of 'otherness', which creates separatist culture.
- The diverse nature of India, being multi-religious and multi-ethnic, is not immune to radicalization.
- Radicalization has spread in India, resulting in violence and separatist movements.
- Social disintegration occurs due to various factors such as Left-Wing Extremism.
- An atmosphere of fear, suspicion and panic is also created due to various factors.

Political-Administrative Challenges

- **Center-state relations** can be a source of tension and conflict, affecting national integration.
    - Demands for greater state autonomy can create friction.
    - **Over-centralization** and authoritarianism damages the fabric of unity.
    - States have felt sidelined, which undermines national integration.
    - Disputes over land and resources can lead to conflicts.
- **Political polarization** and a lack of consensus can hinder national unity.
    - People and political parties are often divided on various issues.
    - Political parties can manipulate religion, resulting in communal conflict.
    - The rise of regional political parties can also create divisions.
    - **Communalism**, **regionalism** and **casteism** are used by political actors.
- **Governance issues** in diverse regions create challenges for national integration.
    - The Northeast region has faced issues of insurgency and underdevelopment.
    - There are sub-regional conflicts and ethnic tensions in this region.
    - Lack of proper implementation of PESA has caused resentment in scheduled areas.
    - The government's administrative approach has exacerbated the region's violence.
    - Poor development in the Northeast makes it a hotbed for insurgency.
    - The lack of representation in power structures also contributes to conflict.
    - **Corruption** is also a major issue and causes popular dissatisfaction.
- **The Armed Forces Special Powers Act (AFSPA)** is a contentious issue.
    - Its prolonged use has led to human rights violations in disturbed areas.
    - It is seen as a tool to deal with extraordinary law and order situations.
    - It is also deemed necessary to prevent security gaps.
- **Border management** is complex and poses challenges to national integration.
    - Porous borders, difficult terrain, and lack of cooperation are some challenges.
    - Cross-border movement of insurgents creates security challenges.
    - The presence of terrorist groups in border regions also threatens security.
    - **Illegal immigration** and demographic changes create social tensions.
    - The **lack of a definite refugee policy** also creates problems.
- **Internal Security** is impacted by issues like terrorism and left wing extremism.
    - These security issues not only hurt the law & order situation inside the country but also hurt developmental gains.
- **Data-led governance** is essential to ensure effective policy making.
    - There needs to be effective collection of data at the local and national levels.
    - Data must be accurate, timely and of good quality for effective governance.
- **The lack of a national security doctrine** and a national security policy is a problem.
    - There is lack of political consensus on national security matters.
    - The need for a National Security Strategy is essential to deal with evolving security challenges.

    - Coordination between different agencies responsible for security needs to be improved.
- **The Panchayati Extension to Scheduled Areas Act (PESA)** was created to address the problem of self-governance.
    - However the implementation of the Act has not been sufficient.
- There is a need to **strengthen the capabilities of security forces** while also respecting human rights.
    - It is also necessary to address the grievances of the people through development initiatives.
- **The National Investigation Agency (NIA)** is a positive move in the right direction.
    - However, there are also human rights concerns regarding its methods.

Economic challenges

- **Regional economic disparities** significantly affect national integration.
    - Economic gaps cause resentment and a sense of injustice in less developed areas.
    - Exploitation of natural resources without regard for indigenous people exacerbates issues.
    - The North East region is considered one of the most ignored areas in terms of development.
    - There is a need to minimize regional disparities and involve all sections of society.
- **Resource distribution issues** can lead to conflict and hinder national unity.
    - Disputes over land and water resources create friction between states and communities.
    - Uneven access to resources contributes to social and economic inequalities.
    - The demands of tribal communities like Naga, Kuki, and Manipuri for resources have not been met.
    - There is a need to look at land transfer issues in affected areas to resolve conflict.
- **Development imbalances** across different regions pose a serious challenge.
    - Scarcity of development and education are major factors in the spread of Left-Wing Extremism.
    - Underdevelopment and poverty make it easier for insurgents to recruit youth.
    - The lack of economic opportunities can push people toward illegal activities.
    - The lack of employment opportunities can create a breeding ground for radicalization.
    - Poor infrastructure in border areas impacts overall development.
- **Illegal activities** impact the economic health of the nation.
    - Drug trafficking and human trafficking are a continuing threat to the economy.
    - Organized crime networks use illicit money to fund terrorist activities.
    - Money laundering, often linked to crime, is also a threat to the nation's economy.
    - The use of counterfeit currency harms the economy and creates a black money market.
- **The lack of a skilled workforce** also contributes to developmental imbalances.
    - There is a need to focus on skill development and training to enhance employability.
    - Initiatives like 'UdDAAN' provide skills to dropouts.
- **The lack of adequate infrastructure** in some areas hinders economic growth and integration.
    - Poor connectivity in the Northeast region needs to be addressed through transit treaties.
    - Infrastructure development in border regions is essential for economic activity.
- **The presence of a parallel economy** also poses challenges.
    - This black money fuels corruption and criminal activities in the country.
    - There is a need to improve the system of tax collection and revenue generation.
- **Economic growth** needs to be inclusive and benefit all sections of society.
    - The government needs to ensure that the fruits of economic development are shared equally.

    - Socio-economic development is essential for preventing people from falling prey to propaganda.
- **The need to enhance manufacturing capabilities** and boost economic growth.
    - The government is taking measures to boost the manufacturing sector in the country.
- **The agricultural sector also needs attention** to enhance productivity and farmer incomes.
    - Schemes like PM-KISAN aim to support farmers with financial assistance.
- **The informal economy** also has an impact on the overall economy.
    - There is a need to formalize more sectors of the economy.
- **The need to bridge the digital divide** in the country and provide more access to technology.
    - There is a need to promote the use of technology in all sectors of the economy.
- **The lack of access to finance** also hinders economic development.
    - There is a need to improve access to finance and credit for businesses.

National Integration Council (NIC)

- The **National Integration Council (NIC)** is an extra-constitutional body aimed at national integration.
    - It was established in 1961 to combat communalism, casteism, regionalism, and linguism.
- The NIC is chaired by the Prime Minister of India.
- The composition includes Union cabinet ministers, chief ministers, political leaders, and academics.
    - Representatives from industry, business, and trade unions are also members.
- The NIC's objectives include promoting common citizenship, unity in diversity, and secularism.
    - It seeks to achieve equality, justice, and fraternity among all communities.
- The council aims to address issues that threaten national solidarity.
    - It discourages communal ill-will, regional animosities, and violence.
    - It also promotes tolerance and harmony.
- The NIC has held sixteen meetings, with the first in 1962.
    - The most recent meeting was in 2013, which focused on communal peace and atrocities.
- The NIC's major purpose is to investigate national integration and give recommendations.
- **A critical evaluation reveals the NIC has faced challenges in achieving its goals**.
    - There is a need to address issues like regionalism, communalism, and casteism that still persist.
    - There is also a need to address the political polarization that exists in the country.
- The council's effectiveness is also limited by the lack of a definite policy for national integration.
    - There is a need for a more proactive approach to promote national unity.
- The NIC needs to be more active and responsive to the current challenges facing the nation.
- The NIC is also not a statutory body, which limits its power and influence.
- There is a need for a strong and sustained effort to promote national integration.
- The NIC has also been criticized for being ineffective and a mere talking shop.
- The **Kargil Review Committee (KRC)** was set up to look into lapses in national security.
    - It was formed after the Kargil War in 1999 to give recommendations on national security.
    - It examined areas like intelligence, border management, and defense procurement.
- The **National Security Council (NSC)** considers all aspects of national security.
    - The Prime Minister serves as the head of the NSC.
    - It is an apex body that deliberates on national security.
- The **National Security Advisory Board (NSAB)** advises the NSC.

    - The NSAB consists of experts in various fields.
- There is a need to recognize India's national security concerns and take realistic measures.
- There is also a need for a national security strategy to tackle evolving security challenges.
- The **Defense Planning Committee (DPC)** is tasked with preparing a draft national security strategy.
- The **Hooda Committee** also suggested tenets for a draft National Security Strategy.

Hooda Committee Suggestions for a Draft National Security Strategy (NSS)

The Hooda Committee, established in 2018, provided key tenets for drafting a comprehensive National Security Strategy (NSS) to address evolving security challenges and enhance India's defense capabilities.

- **Assuming India's Rightful Place in Global Affairs**: This tenet emphasizes that India should aim to play a significant and influential role on the global stage.
- **Achieving a Secure Neighborhood**: The committee highlighted the importance of fostering cooperation and stability in India's surrounding region.
- **Peaceful Resolution of Internal Conflicts**: The strategy should prioritize integrating the North East, and actively combatting terrorism within the country.
- **Protecting the People**: This involves ensuring economic security, managing cyber threats, and addressing climate change to safeguard the well-being of India's population.
- **Strengthening Capabilities**: The committee stressed the need to enhance India's maritime borders, space capabilities, and strategic communications infrastructure.

Kargil Review Committee (KRC):

- While primarily focused on national security, the KRC also touched on aspects relevant to national integration. The committee recommended strengthening the National Security Council (NSC) and having a full-time National Security Advisor (NSA). It also suggested creating civil-military liaison mechanisms at various levels to promote better relationships between the military and the media, which can enhance national unity

Madhukar Gupta Committee

The **Madhukar Gupta Committee** made recommendations on border management, which are critical for national security and integration. These recommendations include:

- **Comprehensive Border Management:** Implementing comprehensive strategies, including **fencing, 24x7 surveillance**, and the use of new imaging technology for enhanced border security.
- **Technology Integration:** Employing modern technology for the protection of borders, as technology plays a key role in effective border management. This includes the use of sensors at borders.
- **Border Infrastructure:** Strengthening border infrastructure is essential for effective border management. This involves constructing roads, communication networks, and other necessary facilities to support security forces and improve surveillance.
- **Strategic Deployment:** Ensuring strategic deployment of forces is crucial to prevent infiltration. This involves positioning security personnel at vulnerable points and using technology for effective monitoring.
- **Intelligence and Analysis:** The committee also stressed the need to improve intelligence gathering and analysis capabilities. This includes using both human intelligence (HUMINT) and technological intelligence (TECHINT) for better threat assessment.

National Integration: Solutions and Way Forward

- **Policy Measures**
    - **Constitutional provisions** should be effectively implemented to promote equality and social justice.
        - Article 244 (2) of the 6th Schedule allows for Autonomous Councils with powers.

- **Border management** needs comprehensive strategies including fencing and surveillance using technology.
    - The Madhukar Gupta Committee's recommendations on border management should be implemented.
- **Refugee policy** needs to be formulated to provide basic rights and end uncertainty for excluded individuals.
    - Consideration should be given to the right to work and identity cards.
- **Address alienation** by creating awareness programs that debunk misleading propaganda.
- **Strengthen intelligence** to track recruitment attempts by Over Ground Workers (OGWs).
- **Promote economic development** in underdeveloped areas to reduce regional disparities.
    - Targeted investments in infrastructure such as roads, railways, and communication are essential.
- **Improve connectivity** to ensure access to employment and modern education, especially in tribal areas.
    - Technology penetration in tribal regions is needed, including access to electricity and cell phones.
- **Enhance infrastructure** by building bridges and transportation networks in the North East region.
    - The inauguration of the Daporijo Bridge and the Bogibeel Bridge are examples of initiatives.
- **Implement schemes** to ensure fair resource sharing and social infrastructure development.
- **Address grievances** of marginalized groups to prevent their exploitation by insurgent groups.
- **Special focus** should be given to the North East region to address its unique challenges.
    - The Bezbaruah Committee recommended increased representation in the central government.
- **Promote entrepreneurship** and start-ups in the North East through the NE Venture Capital Fund.
- **Utilize science and technology** to improve the lives of farmers and artisans in the North East through STINER.

Social Reforms

- **Promote secularism** by emphasizing the common identity of all citizens, despite religious or cultural differences.
    - The Constitution declares India to be a secular state.
- **Combat communalism**, which is a threat to national integration.
    - It is important to address the root causes and manifestations of communalism.
- **Promote interfaith dialogue** and cohesion to break down social barriers.
    - This will also address the concerns of minority groups and improve trust among communities.
- **Eradicate casteism** by emphasizing equality, social justice, and access to opportunities for all.
- **Address regionalism** by ensuring balanced development and promoting national integration.
    - National integration is critical for cultural and religious diversity.
- **Improve education** to promote a sense of unity and national identity among all citizens.
    - Education can help in changing the perception of people towards other regions.

- **Encourage cultural exchange** to foster a feeling of oneness among citizens from different states.
    - This would increase awareness and respect for the diverse cultural heritage of India.
- **Promote awareness** through programs like Destination North East (DNE) and Azadi ka Amrit Mahotsav (AKAM).
- **Engage youth** in activities that foster national unity and a sense of common identity.
- **Address social injustices** to reduce the chances of youth joining insurgent groups in the North East.

Economic Initiatives

- **Promote balanced regional development** to minimize disparities and address grievances.
    - Economic growth should involve all sections of society.
- **Invest in infrastructure** in underdeveloped regions to create employment opportunities and connectivity.
    - Targeted infrastructure development should include roads, railways, and communication networks.
- **Develop industrial infrastructure** to generate employment in backward areas and curb migration.
- **Address unemployment** through skill development and entrepreneurship programs.
    - The NE Venture Capital Fund can empower entrepreneurs and encourage start-ups in the North East.
- **Provide access to credit** and financial inclusion to marginalized communities to boost economic activities.
- **Ensure fair distribution of resources** and address economic exploitation, especially in tribal areas.
    - Government should take initiatives to ensure social and economic development.
- **Use technology to enhance agriculture** and support traditional industries in rural areas.
    - The Science and Technology Interventions in North East (STINER) program aims to bring relevant technologies to farmers/artisans.
- **Encourage local industries** and small businesses through government support and policies.
- **Increase technology penetration** in tribal regions, including access to electricity and cell phones.

Administrative Steps

- **Strengthen local governance** by devolving powers to local bodies and ensuring their effective functioning.
    - The Panchayat Extension Scheduled Areas Act, 1996 (PESA) allows for self-governance in Scheduled Areas.
- **Improve coordination** among various government agencies to ensure effective policy implementation.
    - There is a need for a security-oriented approach with better coordination between police and intelligence agencies.
- **Streamline the administration** in the North East to reduce alienation and promote integration.
    - The Bezbaruah Committee recommended increased representation of North-easterners in the central government.
- **Enhance border security** to prevent illegal immigration and cross-border crimes.
    - Implement the Madhukar Gupta Committee recommendations on border management.

- **Address grievances** promptly through effective redressal mechanisms to build trust and confidence.
- **Conduct regular reviews** of administrative systems to identify gaps and improve performance.
    - The system of official inspections and reviews of organizational performance must be revitalized.
- **Improve intelligence gathering** and surveillance to track and prevent anti-national activities.
- **Promote transparency** and accountability in governance to reduce corruption and improve efficiency.
- **Ensure fair representation** of all communities in government bodies and decision-making processes.
- A lack of representation in power structures contributes to the culture of political unrest in the North East.
- **Enhance the capacity of security forces** to maintain law and order while respecting human rights.
    - The Armed Forces Special Powers Act (AFSPA) should be reviewed periodically to minimize human rights abuses.

Role of Civil Society

- **Promote communal harmony** and counter divisive forces through interfaith dialogues and peace initiatives.
    - The National Integration Council (NIC) aims to promote communal peace and eradicate atrocities against Scheduled Castes and Tribes.
- **Engage in awareness programs** to educate people about the importance of unity and diversity.
    - Destination North East (DNE) and Azadi ka Amrit Mahotsav (AKAM) are examples of awareness programs on the North East region.
- **Facilitate dialogue** between different ethnic and religious groups to resolve conflicts and build trust.
- **Encourage cultural exchange** programs to foster mutual understanding and respect among communities.
- **Support inclusive education** to promote values of tolerance and empathy among children.
- **Mobilize communities** to participate in development initiatives and promote social inclusion.
- **Monitor and report** human rights violations and advocate for justice for marginalized groups.
- **Provide support** to victims of conflict and violence, promoting reconciliation and healing.
    - Civil society can help rehabilitate orphans, counteracting the influence of over-ground workers.
- **Counter fake news** and misinformation to prevent the spread of hatred and violence.
- Users should question the source and credibility of content before sharing it.
- **Promote responsible media** and discourage sensationalism to enhance social harmony.
- The media should avoid spreading misinformation and must be wary of cyber indoctrination.
- **Engage in advocacy** for policy changes to address inequalities and promote social justice.
- **Foster a sense of national identity** based on shared values, common citizenship, and respect for diversity.
    - National integration is critical for a country like India with diverse cultural and linguistic identities.

    - **Act as a bridge** between the government and the people, facilitating effective policy implementation.
    - **Encourage participation** in volunteer activities to strengthen national unity.

National Integration Scheme

- **Vibrant Villages Programme (VVP):** This centrally sponsored scheme provides funds for the development of essential infrastructure and the creation of livelihood opportunities along the northern land border. It covers Himachal Pradesh, Uttarakhand, Arunachal Pradesh, Sikkim, and Ladakh. The VVP aims to improve the quality of life of people in these regions and reverse out-migration, thereby enhancing border security.
- **Border Area Development Programme (BADP):** This program, implemented through state governments and union territory administrations, focuses on habitation areas within 0-10 kilometers of the international border. It funds projects related to village infrastructure such as roads, bridges, healthcare, and education.
- **Border Infrastructure and Management (BIM) Scheme:** Designed to strengthen border infrastructure, this scheme enhances border management and facilitates effective border policing to improve border security.
- **Comprehensive Integrated Border Management System (CIBMS):** This initiative uses non-physical barriers to manage borders where physical fences are not feasible. It integrates manpower, sensors, networks, intelligence, and Command & Control Solutions to improve situational awareness and decision making.
- **National Policy for Drug Demand Reduction:** Implemented by the Ministry of Social Justice and Empowerment, this policy aims to reduce addiction among people.
- **National Integration Council (NIC):** Established to review matters pertaining to national integration and make recommendations, the NIC emphasizes common citizenship, unity in diversity, freedom of religions, secularism, equality, justice, and fraternity. The NIC also mobilizes constructive forces of society for national unity and solidarity.
- **National Festivals and Symbols:** National festivals like Independence Day and Republic Day, and national symbols such as the National Flag and National Anthem, are promoted as unifying forces.
- **All India Services:** The All India Services (IAS, IFS, IPS) and the unified judicial system, as well as postal and communication networks, promote the unity and integrity of the Indian nation.
- **Pradhan Mantri Jan Vikas Karyakram (PMJVK):** A centrally sponsored scheme aimed at the socio-economic development of areas with development deficits, focusing on minority communities. It seeks to develop infrastructure projects and provide basic amenities in identified minority concentration areas.
- **Rashtriya Gram Swaraj Abhiyan (RGSA):** This scheme seeks to develop the governance capabilities of Panchayati Raj Institutions (PRIs) by enhancing their effectiveness and promoting devolution of powers and responsibilities.
- **National Programme for Civil Services Capacity Building (NPCSCB) - Mission Karmayogi:** Aims to transform the Indian civil services capacity building landscape through continuous learning to make officials future-ready.
- **Skill India Programme:** Aims to improve short-term skill training through strengthening institutions and bringing better market connectivity.
- **Pradhan Mantri Adi Adarsh Gram Yojana (PMAAGY):** This centrally sponsored scheme aims to transform villages with significant tribal populations into model villages by improving infrastructure and maximizing the benefits of government schemes.
- **Pradhan Mantri Janjati Adivasi Nyaya Maha Abhiyan (PM JANMAN):** Launched to focus on the development of Particularly Vulnerable Tribal Groups (PVTGs), this initiative converges various ministries to ensure the delivery of essential services and infrastructure.
- **Eklavya Model Residential Schools (EMRS):** This central sector scheme aims to provide quality education to Scheduled Tribe (ST) children in remote areas.
- **Mission Vatsalya:** Aims to provide support for children in difficult circumstances, focusing on ensuring their well-being, care and protection.

- **Khelo India:** A central sector scheme aimed at promoting mass participation and excellence in sports.

These schemes, combined with initiatives focusing on education, health, and economic development, represent the government's multi-faceted approach to promoting national integration and ensuring a unified, prosperous India.

Challenges to internal security through communication networks, Role of media and social networking sites in internal security challenges....1
Internal Security Challenges: Communication Networks and Social Media....1
● Understanding Communication Networks and Modern Media....1
Exploitation of Technologies for Security Threats....2
Cyber Security Threats....3
Social Media and Security Implications....4
Cloud Computing and Government Security....5
Non-State Actors and Subversive Activities....6
Case Studies: Non-State Actors, Subversive Activities, and Cyber Threats....7
Technical Measures....8
Policy Measures....9

Challenges to internal security through communication networks, Role of media and social networking sites in internal security challenges

Internal Security Challenges: Communication Networks and Social Media

- **Understanding Communication Networks and Modern Media**
  - **Communication networks interconnect electronic devices** for transmitting data, voice, and video using hardware and software.
    - Infrastructure includes mobiles, laptops, sensors, servers, and satellites.
  - **Critical Information Infrastructure (CII)** comprises resources which impact national security, economy, or public health if incapacitated.
    - Section 70 of the IT Act 2000 defines CII.
  - **The internet** and **social media platforms** enable information sharing and interaction among users.
    - Social media platforms include Facebook and Twitter.
  - **Cloud computing** allows data and software to be stored and accessed over the internet, which can have security implications.
    - Cloud hosting versus in-house hosting has implications for government businesses.
  - **Cybersecurity** is crucial for protecting systems and information from digital attacks in cyberspace.
    - Cybersecurity is critical for governance, defense, and financial systems.
  - **Social media has become a tool for information warfare**, to propagate ideology, and to conduct psychological operations.
    - Terrorist organizations use social media platforms for propaganda and recruitment.
  - **Fake news** is deliberately disseminated misinformation that can create social disruption.
    - A recent survey shows 64% of Indians have encountered fake news.
  - **Artificial intelligence (AI)** and **machine learning (ML)** are used to identify and predict digital attacks.
    - AI can help form databases of accounts known for spreading fake news.
  - **Drones** are a part of modern warfare and can be used for surveillance and attacks.
    - Drones can transport small arms across the border.

        - Even used in Drug Transport (PJ)
    - **The National Cyber Security Policy 2013** was created to establish a secure cyber ecosystem and enhance the adoption of IT.
        - A new National Cyber Security Strategy was conceptualized in 2020 by the Data Security Council of India (DSCI).
    - **CERT-In** is responsible for responding to computer security incidents and vulnerabilities in Indian cyberspace.
        - It issues directions to secure cyberspace.
    - **The National Cyber Coordination Centre (NCCC)** is responsible for situational awareness and sharing information related to cyber threats.

Exploitation of Technologies for Security Threats

- **Cyber Espionage:** Communication networks can be exploited to obtain secret information from individuals, competitors, or governments using malicious software like Trojan horses and spyware. This includes personal, sensitive, and classified data, potentially harming national security.
- **Cyber Attacks:** Computer systems, infrastructures, and networks can be targeted to damage or disrupt operations. Such attacks can lead to the destruction of communication networks.
    - **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks** make websites and servers unavailable by overwhelming them with traffic.
    - **Ransomware** can limit access to computer systems and encrypt data, demanding payment for its release.
    - **Buffer overflow** bugs in programs can allow attackers to control system execution.
    - **Man-in-the-middle (MitM) attacks** intercept communication between systems or people to steal data.
    - **Malware**, including viruses, worms, and Trojans, can steal, encrypt, or delete data.
    - **Phishing and spear phishing** techniques can be used to trick users into revealing personal and financial information.
- **Cyber Terrorism:** Terrorists use cyberspace to plan attacks, recruit members, spread propaganda, and raise funds. They use online platforms to radicalize individuals.
    - **Social media** is used for propaganda, recruitment, and communication among terrorist groups.
    - **Online radicalization** leads to the transformation of individuals into violent extremists.
    - **Dark web** provides anonymity for illegal activities, including the exchange of illegal goods and services.
- **Cyber Warfare:** Countries and their proxies conduct cyber attacks on other nations to steal data, deface websites, or destroy critical infrastructure.
    - **Advanced Persistent Threats (APTs)** are state-sponsored campaigns targeting critical information infrastructure for espionage and data theft.
    - Cyber attacks can destabilize nations.
- **Use of AI in Cyberattacks**:
    - AI is used by hackers to craft realistic phishing emails.
    - AI is used to generate new types of malware that can evade security systems.
    - AI tools are used to collect and analyze large volumes of data for malicious purposes.
- **Drones:** These are easily accessible tools that can be exploited for terrorist attacks and smuggling.
    - Drones can be used for surveillance, reconnaissance, and attacks.
    - Drones can transport weapons, drugs, and other contraband across borders.
    - Rogue drones can impact civilian airspace and critical infrastructure.
- **Social Media Exploitation:**
    - Social media platforms spread fake news and hate speech to create social discord.

    - Non-state actors use social media to coordinate protests and events, and to raise funds.
- **5G Vulnerabilities:**
    - 5G networks are vulnerable to mobile network mapping attacks, where attackers can gather information from devices on the network.
    - 5G technology relies on shared infrastructure and could be subject to mass failure due to a successful attack on a linked network.
- **Other Threats:**
    - **IP spoofing**, where an attacker pretends to be a trusted computer.
    - **Crypto-jacking**, where malware uses a victim's computer to mine cryptocurrency.
    - **Social engineering** techniques manipulate users to provide confidential information.
    - **Information warfare** disrupts the flow of reliable information.

Cyber Security Threats.

- **Ransomware Attacks:** India has faced multiple ransomware attacks. In 2017, the **WannaCry and Petya ransomware** attacks impacted systems. In 2021, a report indicated that one in four Indian organizations suffered a ransomware attack. Maharashtra was particularly targeted, facing 42% of all ransomware attacks in India in 2021. Additionally, a report from GajShield indicated a significant rise in reported ransomware attacks across businesses in India, due to the sophisticated use of AI within these attacks.
- **Data Breaches:** Several data breaches have compromised sensitive information. In 2018, the **Aadhaar software was hacked**, leading to the leakage of Aadhaar details online. There have been other significant breaches, including:
    - The personal information of approximately 1.5 million customers of Taj Hotels was potentially compromised.
    - In 2023, personally identifiable information of 815 million Indian citizens, including Aadhaar numbers and passport details, were reportedly being sold on the dark web.
    - Data of Indian citizens who registered with the CoWIN portal for vaccination purposes was leaked.
    - A data breach at the RailYatri ticketing platform occurred in December 2022.
    - A recent MOVEit cyberattack, and data breaches at Boeing and AADHAR also occured.
    - Credit card information of 40 million Indian citizens was leaked recently.
- **Pegasus Spyware:** The **Pegasus spyware issue** in 2021 involved the use of surveillance spyware to target mobile phones, raising concerns about privacy and government surveillance. This spyware, developed by the Israeli company NSO, can read messages, calls, and remotely record conversations without the target's knowledge. It is considered a weapon and has been used by governments to surveil political opponents, raising questions about surveillance laws in India.
- **Cyber Attacks on Critical Infrastructure:** There have been attacks on critical information infrastructure. A **Chinese cyber-attack on the power system in Mumbai** brought the city to a standstill. A malware attack was detected at the All-India Institute of Medical Sciences (AIIMS) in New Delhi. In 2020, there was also a cybersecurity breach at the Kundankulam Nuclear Power Plant.
    - The Stuxnet worm attack on Iranian nuclear facilities led to the destruction of equipment controlled by computers.
- **Phishing and Malware Attacks:** Various forms of phishing and malware attacks have been reported. A banking trojan known as Cerberus has taken advantage of the COVID-19 pandemic by sending SMS messages with links to malicious software. There are also threats from viruses and trojan horse applications, which can harm end-user computers. Additionally, there is a rise in AI-powered attacks that generate convincing phishing emails.
- **Other cyber security incidents**

    - During the G-20 summit in 2023, the official website was targeted by 16 lakh cyber attacks per minute.
- India's financial sector faced more than 13 lakh cyber-attacks between January and October 2023.
- Cybercrime reporting surged by 24.4% in 2022, totaling 65,893 cases.
- There were 48,285 government-related cyber security incidents reported by CERT-In in 2021.
- In 2024, there were reports of ransomware attacks in Bengaluru.
- In 2023, 17,000 Wordpress sites were hacked.
- **Digital Arrest Scams:** Recently, CERT-In issued an advisory about digital arrest scams, where fraudsters impersonate law enforcement officials to extort money. Indians lost ₹120.30 crore in digital arrest scams from January to April of this year. Many of the perpetrators of these scams are based in Myanmar, Laos and Cambodia.

Social Media and Security Implications

- Social media are web-based platforms that enable user interaction and content sharing.
    - Platforms include blogs, wikis, discussion forums, and social networking sites.
- Social media has become ubiquitous, with significant influence on modern life.
    - **Over half of Indians, 759 million citizens, are active internet users**.
    - **399 million users are from rural India and 360 million from urban areas**.
    - Active internet users are projected to reach 900 million by 2025.
- Social media platforms have both benefits and security vulnerabilities.
    - Benefits include increased interactivity and user engagement.
    - Risks include cyber terrorism, fraud, criminality, and propaganda.
- Social media is exploited for propaganda, recruitment, and communication among terrorist groups.
    - **Online radicalization** leads to the transformation of individuals into violent extremists.
- Social media is used to spread fake news and disinformation, creating social discord.
    - **64% of Indians surveyed have encountered fake news**.
    - Fake news can manipulate elections and incite violence.
- Non-state actors use social media to coordinate protests, events, and raise funds.
    - Non-state actors can influence or impact state institutions.
- Social media platforms can be used for cyberstalking, cyberbullying, and identity theft.
    - **Data breaches** can compromise sensitive personal and financial information.
- Social media can be used to carry out invisible warfare through misinformation and perception.
    - Invisible warfare is fought with soft forces like diplomacy and cyber attacks.
- Social media can be a source of digital security attacks and breaches.
    - **AI and machine learning** can help predict and identify digital security threats.
- Social media platforms, along with encrypted messaging, are used to conduct covert communications.
    - Terrorists use various online avenues for communication.
- Social media platforms are used to spread hate speech and incite violence.
    - **Social media has a high concentration of online security vulnerabilities**.
- The use of social media for subversive activities is a significant security concern.
    - Guidelines are needed to curb threats from misuse of social media.
- Lack of awareness of security issues related to digital communication networks increases risk.
- Users need more awareness about security regarding digital communications, devices and services.
- The government is taking steps to manage these threats.
    - **Sectoral Cyber Security Incident Response Systems (CSIRT)** are being established.
    - Information sharing between security agencies needs improvement.

- **India was ranked 159 out of 180 in the World Press Freedom Index**.
    - Biased reporting and fake news are negative impacts of the media.
- Social media platforms have become a venue for internal security issues.
    - Social media is a place where cyber terrorism takes place.
- Social media is used to spread propaganda, impact psychological warfare, and recruit new members.
- Terrorist groups use online magazines and videos to spread their ideology.
- Radicalization is the transformation of individuals into violent extremists.
    - It is the process by which people come to support terrorism and extremism.
- Users should question the source and credibility of content before sharing.
- Users should verify the credentials of the individual it has come from.
- A database of known fake news sources should be formed to help with A.I. detection.
    - Specific accounts, sources, geographical locations and IP addresses can be used to identify fake news.
- While technical measures are important, they are not sufficient to address the political problem posed by fake news.
- The spread of fake news requires more than just technical intervention.
- **The digital divide continues to plague the country with Bihar having only 32% internet users**.
    - This digital divide limits the reach of cyber security information and awareness programs.

Cloud Computing and Government Security

- Cloud hosting services provide virtual servers that access computational resources via web networks.
    - It offers utility model of computing, on-demand payment for resources used.
- In-house hosting maintains its own servers and infrastructure on premise.
    - **Cloud based hosting** maintains its servers remotely.
- Cloud hosting offers benefits like scalability, flexibility, and cost-effectiveness.
    - Suited for fast expanding firms and organizations.
    - **Businesses can scale up or down resources** as needed and pay for only what is used.
- Cloud access allows workers to connect from any device, anywhere, increasing flexibility.
    - Bring your own device policies can be implemented in businesses.
- Cloud data can be backed up with minimal risk of data loss.
    - Data can be backed up on the cloud at as little as 15 minute intervals.
- In-house hosting provides physical access to the server and control over sensitive data.
    - Keeps data in-house, so no one else has access to it.
- In-house hosting may require less reliance on internet connection.
    - Companies concerned with uptime may find it more cost-effective.
- Cloud hosting has security implications because all traffic must pass over the internet.
    - Internet connections need to be protected.
- Data on a cloud provider's server is viewed by the cloud company.
    - The data owner has no control over the provider's personnel.
- **Cloud hosting has potential security risks regarding access and data breaches.**
    - Security measures must be in place to ensure data is encrypted.
- The government has made strides in promoting a secure cyber ecosystem.
- **The National Cyber Security Policy, 2013** was formulated for a secure cyber ecosystem.
- A new National Cyber Security Strategy was conceptualized by the Data Security Council of India (DSCI) in 2020.
    - **This strategy aims to enhance adoption of IT in all sectors of the economy.**
- A cybersecurity board with government and private sector is needed for better cybersecurity.

    - This board should have the authority to make recommendations.
- **Quantum-resistant communications need to be developed for critical strategic sectors.**
    - The Indian defense establishment should emulate cryptographic standards like NIST.
- **The National Cyber Security Policy, 2013** is intended to safeguard sensitive information.
    - This includes personal, financial, banking and sovereign data.
- The policy intends to protect public and private infrastructure from cyber-attacks.
    - Security standards need to be defined for government and private organizations.
- **The National Cyber Security Strategy** focuses on 21 areas for a safe cyberspace.
    - This strategy was prepared by the Data Security Council of India.
- The government is working on a new Cyber Security Policy.
    - The existing IT Act and NCSP, 2013 are outdated.
- The government is working to improve the cyber security ecosystem.
    - Tax incentives can be provided to upgrade infrastructure.
- **The National Cybercrime Reporting Portal** is a citizen-centric initiative to report cybercrime.
    - It enables victims to report cybercrimes online.
- **The Indian Computer Emergency Response Team (CERT-In)** is the nodal agency for cyber security incidents.
    - CERT-In is responsible for responding to computer security incidents.
- **The National Critical Information Infrastructure Protection Centre (NCIIPC)** works to improve cyber resilience.
    - NCIIPC is designated as the National Nodal Agency for critical infrastructure protection.
- **The Information Security Education and Awareness (ISEA) project** provides training for cyber security.
    - ISEA provides training to personnel to raise awareness about information security.
- The government has also established the **National Cyber Coordination Centre (NCCC)**.
    - The NCCC seeks to generate awareness of potential cyber security threats.

Non-State Actors and Subversive Activities

- Non-state actors operate outside government control and can influence or impact state institutions.
    - These actors can have both positive and negative impacts.
- Non-state actors use communication networks to coordinate events and spread ideologies.
    - Platforms like Facebook, Twitter, YouTube, and WhatsApp are used to communicate.
- Social media is used to disseminate extremist ideologies, fake news, and hate speech by non-state actors.
    - The platforms allow non-state actors to coordinate protests and operations.
- Non-state actors use social media to raise funds online.
    - This can be done through various online payment systems and cryptocurrencies.
- **Cybercrime is a form of subversive activity** used by non-state actors.
    - Cyberattacks can target critical infrastructure and disrupt essential services.
- Non-state actors use the internet for propaganda and to impact public opinion.
    - They use the internet to conduct psychological warfare and to recruit new members.
- **Non-state actors use data mining and analysis to collect information about specific locations and individuals**.
    - This information is used to plan and execute attacks.
- Artificial intelligence (AI) is used by non-state actors to analyze large volumes of data.
    - AI helps them in identifying patterns and vulnerabilities.
- **Terrorist groups use the internet to spread and manage their propaganda**.
    - They use various websites, online magazines, and social media platforms.
- Cyber terrorism involves unlawful attacks against computers and networks.

    - These attacks are intended to intimidate governments or people for political or social objectives.
- **Radicalization is a process by which an individual becomes an active, anti-state, violent extremist**.
    - This can occur through online and offline influence by non-state actors.
- Fake news is deliberately disseminated misinformation or disinformation.
    - It is used to manipulate public perception and create chaos.
- The use of social media for subversive activities is a major security concern.
    - Non-state actors misuse social media to spread extremist ideologies.
- **Invisible warfare is a battle of misinformation and perception using non-kinetic military actions**.
    - It involves soft forces of diplomacy, social engineering, cyber-attacks and sanctions.
- Non-state actors may use media/journalists for biased reporting and spreading fake news.
    - India is ranked low in the World Press Freedom Index.
- Violent non-state terrorism creates instability, radicalizes populations and challenges the authority of government.
    - It is a threat to humanity and infrastructure.
- **Multinational corporations (MNCs) may pose a threat to national security through data and cyberspace**.
    - Data security is a concern with MNC operations.
- **The government has taken steps to counter these threats:**
    - Increasing awareness about security issues related to digital communications.
    - Establishing a Security Incident Management and Response System.
    - Improving information sharing and coordination between various security agencies.

Case Studies: Non-State Actors, Subversive Activities, and Cyber Threats

- **The Role of Social Media in Specific Security Incidents:**
    - **Panchkula Violence:** Social media platforms were used to disseminate extremist ideologies and coordinate protests leading to violence. This demonstrates how non-state actors use social media to mobilize and instigate unrest.
    - **Paris Attacks (2015):** Terrorists coordinated their attacks using social media, highlighting the effectiveness of these platforms for planning and communication. This case underscores how social media facilitates real-time coordination of operations by non-state actors.
    - **Recruitment by ISIS:** Terrorist organizations use social media platforms to recruit new members, spread their propaganda, and manage their operations. This illustrates how social media serves as a crucial tool for radicalization and recruitment.
- **Cyber Espionage on Bharat Biotech and SII:** Chinese hacker group Stone Panda was involved in espionage against Indian vaccine manufacturers during the COVID-19 pandemic. This underscores the threat of state-sponsored cyber espionage.
- **Successful Counter-Measures Against Cyber Threats:**
    - **Cyber Swachhta Kendra:** This platform helps internet users clean their computers and devices by wiping out viruses and malware. This initiative provides a practical tool for improving individual cyber hygiene.
    - **Cyber Surakshit Bharat Initiative**: This initiative aims to spread awareness about cybercrime and build capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across government departments. This highlights the importance of education and capacity-building in countering cyber threats.
    - **National Cybercrime Reporting Portal:** Launched as part of the Indian Cybercrime Coordination Centre (I4C), it enables the public to report incidents of cybercrime.

This demonstrates the government's efforts to improve public awareness and reporting mechanisms.

- **International Best Practices in Cybersecurity:**
  - **Budapest Convention:** While India has not joined this convention, it promotes greater cooperation between countries in fighting cybercrimes. This illustrates the importance of international legal frameworks.
  - Some experts suggest that India should accede to the Budapest Convention to fight cybercrimes.
  - **Bletchley Declaration**: This international agreement aims to address the ethical and security concerns surrounding the use of artificial intelligence, particularly generative AI. This exemplifies global efforts to regulate AI and address ethical challenges.
  - **US's National Institute of Standards and Technology (NIST):** The Indian defense establishment is considering emulating cryptographic standards set by NIST, which has developed tools to handle quantum computer attacks. This showcases an adoption of international standards to address evolving threats.
  - **Global Internet Forum to Counter Terrorism (GIFCT):** This NGO, founded by major tech companies, fosters technical collaboration, advances research, and shares knowledge to counter terrorism online. This demonstrates the importance of public-private partnerships in addressing cyber threats.
  - **Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA):** India may consider similar laws to prevent the circulation of fake news affecting national security. This is an example of how countries address misinformation through legal frameworks.
  - **The Christchurch Call to Action**: India has signed the Christchurch Call to Action, which is an agreement with like-minded countries to counter fake news on an international level. This is a best practice to counter fake news.
  - **Cyber-diplomacy:** The Indian government has entered into cybersecurity collaborations with countries such as the USA, European Union and Malaysia. This demonstrates the need for international collaborations to handle cyber threats.
- **Other Examples**
  - **Maharashtra Social Media Lab:** This lab works 24/7 to keep records of trends in cybercrime and latest techniques used. It shows the need for constant tracking of cyber criminals.

Technical Measures

- **Cybersecurity Infrastructure:**
  - **National Cyber Security Coordinator (NCSC):** The NCSC coordinates with different agencies at the national level for cyber security matters. This helps in creating a unified approach to cyber threats.
  - **National Critical Information Infrastructure Protection Centre (NCIIPC):** The NCIIPC is a national 24/7 mechanism to deal with cyber threats. It aims to improve the security and resilience of critical information infrastructure.
  - **Cyber Swachhta Kendra:** This platform allows internet users to clean their computers and devices by removing viruses and malware.
  - **Botnet Cleaning and Malware Analysis Centre**: This is another function of the Cyber Swachhta Kendra.
  - **CERT-In (Indian Computer Emergency Response Team):** CERT-In functions as a nodal agency for coordination of crisis management efforts, and it also serves as an umbrella organization for coordinating actions and operationalization of sectoral CERTs. It collects, analyzes, and disseminates information on cyber incidents and issues alerts.

    - **Technology Indigenization:** Developing indigenous security technologies through research is a key approach. This will reduce reliance on foreign technology that may be vulnerable to supply chain attacks.
    - **Testing and Validation:** Establishing infrastructure for testing and validating the security of ICT goods and services.
    - **Artificial Intelligence (AI):** Investing in AI and other technologies to identify terror handlers and sources of funding is vital. AI can also be used to detect fake news and extremist content online. AI can be used to create databases of accounts, sources, locations, and IP addresses that are known to spread fake news.
    - **Honey drones (HDs):** These can be used to lure cyber attackers away from critical UAV missions by using lightweight virtual machines to redirect attacks.
    - **Monitoring the internet:** Intelligence services like the Intelligence Bureau and RAW should be used to monitor the internet and prevent any attempts to radicalize teenagers.
- **Social Media and Communication Networks:**
    - **Counter-Narratives:** Developing strategic communications to disseminate political, liberal, and religious counter-narratives to combat the spread of radicalization. This would involve creating narratives that resonate with the local population.
    - **Social Media Monitoring:** Monitoring social media to identify and counter extremist content, narratives, and profiles. Social media should be used to spread messages of peace.
    - **Collaboration with Platforms**: Social media platforms should be encouraged to take responsibility for curbing fake news.
    - **Fact-Checking:** Promoting fact-checking websites and organizations to verify information and combat misinformation.
    - **AI and Blockchain:** Using AI and blockchain to detect and counter financial transactions, fund raising and money laundering by non-state actors.
    - **Messaging App Features:** WhatsApp's "forwarded" sign is a technical measure to help identify messages that are not original.
- **Drone Security:**
    - **Licensing and Registration:** Drones should be registered and licensed to aid in identifying the owners of harmful drones.
    - **Flying Permits:** Issuing flying permits similar to driving licenses.
    - **Multi-factor authentication:** Implementing rigid authentication methods to stop security threats.
    - **Restricted Zones**: Mapping and declaring no-fly zones with public applications.
    - **Private Sector Collaboration:** Encouraging collaboration with the private sector for early detection of threats from non-state actors.

Policy Measures

- **Legal Framework:**
    - **Strengthening IT Act:** The IT Act of 2000 and the National Cyber Security Policy of 2013 need to be strengthened to handle advanced cybercrimes.
    - **Cyber Legislation:** There is a need for cyber legislation at the national level and better cyber-related governance arrangements at firms.
    - **Defining Fake News:** Any amendment to existing laws should start with a definition of fake news.
    - **Special Laws:** Enacting special laws and enforcement mechanisms to deal with terrorists, while ensuring safeguards against misuse.
    - **Data Protection:** Enforcing privacy laws and preventing third parties from sharing user data without consent.
- **Targeted Financial Sanctions (TFS):** Improving the framework for implementing TFS to freeze funds and assets without delay.

- **Governance and Administration:**
    - **Chief Information Security Officer (CISO):** Designating a CISO in all organizations to be responsible for cyber security initiatives.
    - **Public-Private Partnerships (PPP):** Leveraging private sector expertise to combat cybercrimes through PPP frameworks.
    - Developing PPP models to encourage tech start-ups and private industry to work with government agencies.
    - **Risk Management Strategy:** Developing and implementing a cyber risk management strategy to identify threats and put defenses in place.
    - **Cybersecurity Training:** Implementing cybersecurity training programs and providing training to professionals.
    - A national framework for skill development should be devised in collaboration with institutions like the National Skill Development Corporation (NSDC) and the Information Security Education and Awareness (ISEA).
    - **Awareness Campaigns:** Raising awareness among the public about cyber security.
- **Border Management:**
    - **Technology Augmentation:** Augmenting the capabilities of border security forces (BSF) with technology to detect tunnels and drones.
    - **Regulation of Borders:** Effective regulation of the movement of people and goods to prevent illegal migration, smuggling, and infiltration.
    - **Border Infrastructure:** Improving infrastructure to facilitate legitimate trade and travel while preventing illegal activities.
- **Counter-Radicalization:**
    - **De-radicalization Programs:** Developing effective indigenous counter-radicalization programs.
    - **Focus on Families:** Supporting families in preventing and de-radicalizing individuals.
    - **Community Engagement:** Engaging civil society in outreach activities to heal community rifts and tensions.
    - **Education and Employment:** Reemphasizing education and employment opportunities as key to countering violent narratives.
    - **Promote a Liberal Version of Sufi Islam:** Engaging religious scholars in Kashmir to promote a liberal version of Sufi Islam.
- **Media and Information Management:**
    - **Affirmative Media Policy**: Ensuring transparency in governance and advancing media's role as an instrument of vigilance.
    - **Countering Propaganda**: Contradicting extremist content and narratives with consistent counter-narratives.
    - **Media Engagement:** Engaging, enabling, and assisting media to fulfill its role of informed, fair coverage.
    - **International partnerships:** Partnering with countries to counter fake news on an international level. India has signed the Christchurch Call to Action for this purpose.
- **International Cooperation:**
    - **Cyber Diplomacy:** Establishing cybersecurity collaborations with other countries.
    - **Global Legal Framework**: Working with other countries to develop a global legal framework on cyber terrorism.
    - **Budapest Convention:** Considering accession to the Budapest Convention to strengthen international cooperation in fighting cybercrimes.
- **Addressing Root Causes:**
    - **Socio-Economic Development:** Prioritizing socio-economic development to prevent vulnerable sections of society from falling prey to terrorist propaganda.
    - **Good Governance:** Ensuring clean, corruption-free, and accountable administration at all levels.
    - **Addressing Grievances:** Being responsive to the legitimate grievances of people so that they are not exploited by terrorist groups.

    - **Promote Public Trust**: Policies should promote public trust in government to reduce support for non-state actors.
    - **Political consensus:** Political parties must come to a national consensus on a planned strategy.
- **Financial Measures**
    - **Budgetary Provisions**: Setting aside a minimum percentage of the annual budget for cyber security.
    - **Fund of Funds**: Setting up a fund of funds for cyber security and providing central funding to states to build capabilities.

Basics of Cyber Security PYQ **1**
Basics of Cyber Security **1**
Fundamentals of Cyber Security: Definition 1
Key Concepts, Landscape, and Importance 2
1) Key Concepts: CIA Triad, Authentication, Authorization, Non-repudiation 2
2) Cybersecurity Landscape: Trends, Challenges, and Evolving Threats 2
3) Importance of Cybersecurity for Individual, Society, and Nation 3
Types of Cyber Attacks 3
1) Malware 3
2) Phishing & Spear Phishing 4
3) DDoS (Distributed Denial of Service) attacks 4
4) Man-in-the-Middle (MitM) attacks 4
5) SQL Injection attacks 4
6) Zero-day exploits 4
7) Attack Vectors: How are these attacks delivered? 4
8) Impact: What are the consequences of these attacks? 5
9) Emerging Threats: Discuss threats related to emerging technologies like AI, IoT and Cloud 5
Cyber Warfare & Terrorism 6
1) Cyber Warfare Definition 6
2) Cyber Terrorism Definition 6
3) Distinction: Differentiate between cyber warfare, cyber terrorism, and cyber crime 6
4) Geopolitical Dimensions: How do cyber activities affect international relations? 7
5) Impact on National Security: Implications for military operations, critical infrastructure, economic stability 7
Cyber Crime 7
1) Types of Cyber Crime 7
2) Organization of Cyber Criminals 8
3) Motivations 8
4) Cybercrime Ecosystem 8
5) Role of social media and messaging platforms 8
Data Security & Privacy 9
1) Importance of Data Security: Why is data protection crucial? 9
2) Data Privacy vs Data Security: Understanding the difference 9
Information Technology Act, 2000 9
Amendments to the IT Act 9
Important Sections of the IT Act 10
Powers and Functions Under the IT Act 10
Working Mechanism of the IT Act 10
Limitations of the IT Act 11
Digital Personal Data Protection Act, 2023 11
Key Definitions in the DPDP Act 11
Obligations of Data Fiduciaries 12
Rights of Data Principals 12
Special Provisions 12

Amendments to other Acts....12
Powers and Functions of the Data Protection Board of India (DPBI)....12
Working Mechanism of the DPDP Act....12
Limitations of the DPDP Act....13
Cyber Security: Data Security & Privacy....13
1) International Regulations (e.g., GDPR)....13
2) Data Localization: Benefits, drawbacks, and implications....13
3) Challenges: How are the data of citizens and government institutions compromised?... 14
National Cyber Security Policy & Framework (India)....15
1) Key Elements: Goals, initiatives, and approach of the policy....15
2) Institutional Structure: Roles of CERT-In, National Cyber Coordination Centre (NCCC), and other agencies....15
3) Challenges: Implementation gaps, technological limitations, lack of awareness, workforce inadequacies....16
4) Evaluation: Critically evaluate the effectiveness of India's Cyber security policy....16
5) Digital Armed Forces: Need, challenges, and future....17
6) International collaborations: India's cyber security collaborations with other nations... 17
Cyber Security: Social Media & Security....18
Threats & Challenges: Misinformation, propaganda, radicalization, data breaches....18
Impact on National Security: Threat to law and order, social harmony, democracy....18
Counter Measures: Government regulations, fact-checking initiatives, social media companies' responsibilities....19
Ethical Dilemmas: Balancing security with freedom of speech and expression....19
Role of Artificial Intelligence in tackling social media menace....20
Cyber Security Framework & Measures....20
Elements of a Comprehensive Cyber Security Framework: Risk assessment, prevention, detection, response, and recovery....20
Defensive Measures: Firewalls, intrusion detection systems, encryption, security audits, patch management....21
Incident Response: What to do during a cyber attack....21
Cyber hygiene: What is cyber hygiene and how can we promote cyber safety at individual level....22
Role of Technology: How new technologies like AI, ML, Blockchain, Cloud can help in combating cyber threats....22
IoT Security: Vulnerabilities and implications of interconnected devices....23
Cloud Security: Challenges and solutions for securing cloud infrastructure....23
Blockchain: How can it improve security?....23
Quantum Computing and Cyber Security: How is it a game changer and potential threat? 23

Basics of Cyber Security PYQ

- [ ] Answer about Cyber-terrorism. (05/2)
- [ ] Cyber warfare is considered by some defense analysts to be a larger threat than even Al Qaeda or terrorism. What do you understand by Cyber warfare? Outline the cyber threats which India is vulnerable to and bring out the state of the country's preparedness to deal with the same. [200 words) (13/10)
- [ ] Considering the threats cyberspace poses for the country, India needs a "Digital Armed Force" to prevent crimes. Critically evaluate the National Cyber Security Policy, 2013 outlining the challenges perceived in its effective implementation (15/12.5)
- [ ] Discuss the potential threats of Cyber attack and the security framework to prevent it. (2017, 10) Data security has assumed significant importance in the digitized world due to rising cyber-crimes. The Justice B. N. Srikrishna Committee Report addresses issues related to data

security. What, in your view, are the strengths and weaknesses of the Report relating to the protection of personal data in cyberspace? (250 Words 15 Marks)

- [ ] What is CyberDome Project? Explain how it can be useful in controlling internet crimes in India. (2019/10)
- [ ] Discuss different types of cybercrimes and measures required to be taken to fight the menace. (2020/10)
- [ ] Keeping in view India's internal security, analyse the impact of cross-border cyber attacks. Also discuss defensive measures against these sophisticated attacks. (2021/10)
- [ ] What are the different elements of cyber security? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy, (22/15)
- [ ] Social media and encrypting messaging services pose a serious security challenge. What measures have been adopted at various levels to address the security implications of social media? Also suggest any other remedies to address the problem. (Answer in 250 words) 15 marks

Basics of Cyber Security

Fundamentals of Cyber Security: Definition

- Cyber security is protecting information and devices from unauthorized access, use, or destruction.
    - It includes safeguarding computers, networks, and data from cyber threats.
- Cybersecurity is essential due to increasing cyber threats and their impact on national security.
    - Cyber-attacks can disrupt critical infrastructure, cause financial losses, and threaten privacy.
- Cyberspace is a global domain of interdependent information technology infrastructure.
    - It includes the Internet, telecommunications, computer systems, and embedded processors.
- Cyber security is vital for economic stability and national security in a digital world.
    - It protects citizens' data, financial systems, and government infrastructure.
- Cybersecurity addresses threats such as ransomware, cyber espionage, and denial-of-service attacks.
    - Examples of attacks include WannaCry, Petya ransomware, and Aadhaar software hacking.
- Cyber warfare involves using computer technology to disrupt a state's military or strategic operations.
- It involves deliberate assaults on information systems for strategic or military reasons.
- The goal of cyber security is to create a secure cyber ecosystem and ensure trust in IT systems.
    - It also includes enhancing the adoption of IT across all sectors of the economy.
- A strong cyber security framework is necessary for data security and safe digital transactions.
    - It must also include complaint redressal mechanisms.
- Cyber terrorism is the convergence of terrorism and cyberspace.
    - It involves attacks on computer systems to intimidate a government for political objectives.
- Cybersecurity is not limited to government organizations; private companies should also adhere to security standards.
    - A checklist of requirements can be enforced on private companies.
- Cybersecurity includes the functions of identification, protection, detection, response, and recovery.
    - These functions serve as pillars for establishing robust security protocols.
- A comprehensive approach includes raising public awareness and civil society involvement.
    - It's vital to understand that no one is immune from cyber threats.
- Cyber security also encompasses protection from data theft and economic losses due to cybercrime.
- A legislative framework should enable successful cybercrime prevention and prosecution.
- The Information Technology Act of 2000, amended in 2008, is the primary legislation to deal with cybercrimes in India.
    - It provides a legal framework for e-commerce and cyber-terrorism.

Key Concepts, Landscape, and Importance

1) Key Concepts: CIA Triad, Authentication, Authorization, Non-repudiation

- **Confidentiality** ensures that information is accessible only to authorized users.
    - It involves measures like encryption and access controls to protect sensitive data.
- **Integrity** maintains the accuracy and completeness of data, preventing unauthorized modification.
    - Techniques like hashing and checksums ensure that data remains unaltered.
- **Availability** ensures timely and reliable access to information and resources for authorized users.
    - Redundancy and failover mechanisms help maintain service uptime.
- **Authentication** verifies the identity of a user, device, or process attempting access.
    - Passwords, biometrics, and digital certificates are common methods for user authentication.
- **Authorization** determines what an authenticated user is permitted to do or access.
    - Access control lists and role-based access controls are used to enforce permissions.
- **Non-repudiation** ensures that actions cannot be denied by the entity that performed them.
    - Digital signatures and audit trails provide proof of origin and integrity of transactions.

2) Cybersecurity Landscape: Trends, Challenges, and Evolving Threats

- Cyber threats are an emerging concern for India's national security, with increasing cyber attacks.
    - India was the third most vulnerable country in the world in terms of cybersecurity threats.
- **Ransomware** attacks, like WannaCry and Petya, and data breaches, such as the Aadhaar hack, are significant threats.
    - In 2018, Aadhaar software was hacked, and people's data was leaked online.
- **Cyber espionage** involves unauthorized access to sensitive information for strategic advantage.
    - This includes stealing gigabytes of data from financial systems.
- **Denial-of-service (DoS)** attacks disrupt services by overwhelming systems, making them unavailable.
    - These attacks can target websites, causing them to be inaccessible to users.
- **Phishing** involves fraudulent emails to obtain personal and financial information.
    - Botnets are increasingly used to launch phishing attacks.
- **Spear phishing** targets specific individuals or organizations for malicious purposes.
    - IT and ITES companies have increasingly become victims of such targeted attacks.
- Cyber warfare is a growing threat, involving attacks on information systems for strategic advantage.
    - Some analysts consider cyber warfare a bigger threat than terrorism.
- **Cyber terrorism** involves using cyber attacks to intimidate governments for political or social objectives.
    - It is a convergence of terrorism and cyberspace.
- The **lack of a global legal framework** on cyber terrorism poses a challenge.
- There are no specific plans yet to coordinate with other countries.
- **Technological advancements**, including AI and machine learning, create new challenges and opportunities.
    - AI and ML can be used to predict digital security attacks.
- **Data breaches** remain a significant threat and can lead to the loss of sensitive information.
    - A similar data breach occurred in Indian Banks in September 2016, with 3.2 million debit cards exposed.

- **Critical Infrastructure** is vulnerable and can be targeted with cyber attacks.
    - Sectors such as banking, finance, transportation, and power are highly dependent on ICT.

3) Importance of Cybersecurity for Individual, Society, and Nation

- **For individuals,** cybersecurity protects personal data, financial information, and privacy.
    - It reduces the risk of identity theft, financial fraud, and data breaches.
- **For society**, cybersecurity ensures the smooth functioning of critical infrastructure and services.
    - It maintains public safety, trust in digital systems, and economic stability.
- **For the nation,** cybersecurity is vital for national security and economic growth.
    - It protects government infrastructure, defense systems, and strategic assets.
- **Cybersecurity promotes economic stability** by safeguarding financial systems and digital transactions.
    - Cyber attacks can cause huge financial losses for both organizations and the nation.
- A secure cyberspace enables the smooth adoption of digital technologies across various sectors.
    - It also encourages greater trust in IT systems and online transactions.
- **Effective cybersecurity measures** are needed to counter cyber terrorism and cyber warfare.
    - These measures include cyber crisis management plans and incident response systems.
- A strong regulatory framework and national cyber security policies are needed to strengthen cyber security.
    - The National Cyber Security Policy of 2013 provides the vision for protecting national cyberspace.
- Cybersecurity awareness among users is critical to prevent cyber threats.
    - Users should be educated about safe practices and potential cyber threats.
- **International cooperation** is essential to tackle cyber threats and create a safe cyber space.
    - Bilateral agreements with developed nations can promote research and information sharing.
- **Developing a skilled workforce** in cyber security is necessary for robust cyber defense.
    - Educational institutions must offer courses in cyber security.
- **Indigenization of cyber security technologies** enhances a nation's self-reliance and resilience.
    - Developing indigenous security technologies will ensure national digital security.
- The **National Cyber Security Strategy** focuses on 21 areas to ensure a safe, secure, and vibrant cyberspace for India.
    - It recommends allocating a portion of the annual budget for cyber security.

Types of Cyber Attacks

1) Malware

- **Malware** is malicious software designed to damage or gain unauthorized access to systems.
    - It includes viruses, worms, trojans, spyware, and ransomware.
- **Viruses** attach to clean files, spreading to other systems, often causing damage.
    - They can corrupt files, slow down systems, and cause data loss.
- **Worms** replicate themselves and spread through networks, without needing human interaction.
    - The Stuxnet worm attack on Iranian nuclear facilities led to destruction of equipment.
- **Trojans** disguise themselves as legitimate software to gain unauthorized access to systems.

    - They can be used for data theft, espionage, or opening backdoors for further attacks.
- **Spyware** secretly monitors and collects user data, often without their knowledge or consent.
    - This can include tracking browsing habits, keystrokes, and personal information.
- **Ransomware** encrypts user data, demanding payment for its release.
    - The WannaCry and Petya ransomware attacks are examples of significant threats.

2) Phishing & Spear Phishing

- **Phishing** uses fraudulent emails to obtain personal and financial information.
    - Attackers often use official-looking messages to trick victims into revealing sensitive data.
- **Spear phishing** targets specific individuals or organizations for malicious purposes.
    - IT and ITES companies have increasingly become victims of such targeted attacks.

3) DDoS (Distributed Denial of Service) attacks

- **DDoS attacks** overwhelm systems with traffic, making them inaccessible to legitimate users.
    - These attacks can bring down websites and online services.
- **Botnets** are often used to carry out DDoS attacks by using multiple compromised computers.
    - These zombie computers launch attacks without the owners' knowledge.

4) Man-in-the-Middle (MitM) attacks

- **MitM attacks** intercept communication between two parties, potentially altering or stealing data.
    - These attacks exploit real-time processing of transactions and data transfers.

5) SQL Injection attacks

- **SQL injection** attacks exploit vulnerabilities in database systems by injecting malicious SQL code.
    - Attackers use this to gain unauthorized access, modify data or carry out other harmful actions.

6) Zero-day exploits

- **Zero-day exploits** are attacks that take advantage of unknown software vulnerabilities.
    - These attacks occur before a patch or fix is available, making them particularly dangerous.

7) Attack Vectors: How are these attacks delivered?

- Cyber attacks are delivered through various vectors, including **emails, websites, and removable devices**.
    - Phishing emails trick users into revealing information or downloading malware.
- **Compromised software** and applications are used to deliver malicious code to systems.
    - Trojans, for example, are disguised as legitimate software to gain access.
- **Network vulnerabilities** are exploited by attackers to penetrate systems and networks.
    - Worms spread through networks by exploiting such vulnerabilities without user interaction.
- **Social engineering tactics** manipulate users into divulging sensitive information or performing malicious actions.
    - Attackers use psychological manipulation to trick users.
- **AI-powered attacks** use machine learning for sophisticated and automated attacks.
    - These attacks can predict vulnerabilities and adapt to security measures.

- **Zero-day exploits** use previously unknown vulnerabilities to attack systems.
    - These exploits are particularly dangerous as they occur before a patch or fix is available.

8) Impact: What are the consequences of these attacks?

- Cyber attacks cause **financial losses** through theft, fraud, and operational disruptions.
    - Indian organizations have suffered million-dollar losses due to cyber incidents.
- They lead to **reputational damage** for organizations due to data breaches and loss of customer trust.
    - Loss of public trust can significantly affect the credibility of an organization.
- Cyber attacks can compromise **national security** by targeting critical infrastructure.
    - Attacks on power grids, transportation, and communication systems can disrupt essential services.
- These attacks result in **data breaches and privacy violations**, exposing sensitive personal information.
    - Aadhaar data leaks and credit card thefts are examples of such violations.
- There can be **disruption of essential services** such as banking, healthcare and government functions.
    - The Chinese cyber-attack on Mumbai's power system caused a city-wide standstill.
- Cyber attacks can facilitate **espionage** by stealing sensitive government and corporate data.
    - State-sponsored attackers often engage in such activities to gain strategic advantages.

9) Emerging Threats: Discuss threats related to emerging technologies like AI, IoT and Cloud.

- **AI-powered attacks** are becoming more sophisticated, using machine learning to automate and enhance cyber attacks.
    - AI can be used to create highly realistic phishing attempts.
- **IoT devices** present vulnerabilities due to their often weak security features.
    - The large number of interconnected IoT devices expands the attack surface.
- **Cloud environments** face risks due to misconfigurations and unauthorized access.
    - Cloud hosting for government businesses may have security implications.
- There is a rise in **AI-powered social engineering** and deepfake attacks that are difficult to detect.
    - These attacks are used to manipulate users for malicious purposes.
- **Quantum computing** poses threat to traditional encryption methods.
- It requires developing quantum-resistant communications, especially for critical sectors.
- **Ransomware as a service (RaaS)** is emerging as a threat model where cyber criminals sell ransomware tools.
    - This makes it easier for less sophisticated attackers to launch ransomware attacks.

Cyber Warfare & Terrorism

1) Cyber Warfare Definition

- **Cyber warfare** is state-sponsored use of computer technology to attack another nation's systems or networks.
    - It involves deliberate assaults on information systems for strategic or military reasons.
- **State-sponsored attacks** involve governments using cyber means to achieve military or political objectives.
    - These can include attacks on critical infrastructure, espionage, and disinformation campaigns.
- **Cyber espionage** is the act of secretly obtaining confidential information from other nations through cyber means.

    - It involves stealing government, military or corporate data to gain strategic advantages.
- **Propaganda** is the spreading of information, often biased or misleading, through online platforms to influence public opinion.
    - It can be used to destabilize governments or incite unrest.

2) Cyber Terrorism Definition

- **Cyber terrorism** is the convergence of terrorism and cyberspace, involving unlawful attacks on computer systems.
    - These attacks are meant to intimidate or coerce a government for political or social goals.
- **Motivations** for cyber terrorism include political or ideological objectives.
    - Terrorist groups use cyber means to spread fear, disrupt services, and achieve their aims.
- **Targets** of cyber terrorism can include critical infrastructure, government systems, and private sector networks.
    - These attacks can cause significant disruption and harm to a nation's security.
- **Impact** of cyber terrorism can range from disruption of essential services to large-scale economic damage.
    - Cyber attacks can affect the availability, integrity, and confidentiality of data and systems.

3) Distinction: Differentiate between cyber warfare, cyber terrorism, and cyber crime.

- **Cyber warfare** is typically state-sponsored, targeting strategic military or political objectives.
    - It is conducted by nations against other nations and has implications for international relations.
- **Cyber terrorism** is politically motivated, using cyber means to cause fear and disruption.
    - It is usually carried out by non-state actors to achieve political, social, or ideological goals.
- **Cyber crime** is driven by financial gain, targeting individuals or organizations for monetary profit.
    - It includes activities like hacking, phishing, and data theft, with a focus on financial gain.
- **Cyber warfare** is a tool for strategic advantage, whereas **cyber terrorism** aims at creating fear and chaos.
    - **Cyber crime** is primarily for illicit financial gain, often with no political or ideological motive.
- **Cyber warfare** is considered a larger threat than terrorism by some analysts, due to its potential for large-scale impact.
    - The scale and sophistication of cyber warfare attacks pose significant risks to national security.

4) Geopolitical Dimensions: How do cyber activities affect international relations?

- Cyber activities **create tensions** and conflicts between nations, leading to mistrust and instability.
    - State-sponsored cyber attacks can be seen as acts of aggression.
- They lead to **espionage** and theft of sensitive information, creating an environment of suspicion between nations.
    - Cyber espionage can include stealing military, government or corporate data.
- Cyber operations can be used for **political interference**, such as influencing elections or spreading propaganda.

    - This can destabilize governments or incite unrest in other countries.
- **International cooperation** is hindered due to the lack of a global legal framework on cyber activities.
    - There is a need to coordinate with other countries to develop such a framework.
- Cyber activities affect international relations by creating **new forms of warfare** that operate outside traditional norms.
    - Non-kinetic warfare uses cyber, information and psychological tactics.

5) Impact on National Security: Implications for military operations, critical infrastructure, economic stability.

- Cyber attacks can **disrupt military operations** by targeting command, control, and communication systems.
    - They can also compromise defense-related information and communication systems.
- **Critical infrastructure** such as power grids, transportation, and communication networks are vulnerable to cyber attacks.
    - Attacks on these systems can cause significant disruption to essential services.
- Cyber attacks can lead to **economic instability** through theft, fraud, and operational disruptions in financial systems.
    - Cyber incidents have caused financial losses for Indian organizations.
- Cyber activities can **undermine national security** by spreading misinformation and propaganda.
    - This can create social unrest and threaten national unity.
- **Data breaches** and privacy violations expose sensitive personal information, impacting public trust and national security.
    - Aadhaar data leaks and credit card thefts are examples of these violations.
- There is a rise in the use of **drones** in modern warfare, and they are also vulnerable to cyber-attacks.
    - Drones are a key component of modern warfare, but can be hacked and exploited.

Cyber Crime

1) Types of Cyber Crime

- **Financial fraud** involves illegal activities to gain money, such as through online banking, credit card theft, and scams.
    - Cyber fraud constitutes the majority of cybercrime cases.
- **Identity theft** is the act of stealing personal information, used for fraud, impersonation, or other criminal activities.
    - This involves using someone else's personal data without their consent.
- **Online scams** use deceptive practices to trick individuals into giving money or personal information through fake emails or websites.
    - Phishing is a type of scam that tricks people into providing sensitive information.
- **Data breaches** are security incidents that lead to exposure of sensitive information, often due to hacking or system vulnerabilities.
    - These can lead to the leak of personal and financial data.
- **Intellectual property theft** is the stealing of original creative works, designs, or inventions.
    - It includes copyright infringement and counterfeiting.
- **Cyber stalking** is using online platforms to harass or threaten individuals, causing them distress or fear.
    - This can include sending threatening messages or tracking someone's location.

2) Organization of Cyber Criminals

- **Lone actors** are individuals who carry out cyber crimes on their own, often for personal gain or other motives.
    - They may act independently or have a small support network.

- **Criminal groups** are organized networks that engage in sophisticated cyber attacks for financial or other criminal purposes.
    - These groups often use advanced tools and tactics.
- **State-sponsored hackers** are those supported by governments, involved in espionage, sabotage, or other political goals.
    - These activities serve strategic interests of the state.

3) Motivations

- **Financial gain** is a primary motive for cyber crime, involving theft, fraud, and extortion.
    - Cyber criminals aim to profit from data theft and other online crimes.
- **Political activism** can lead to cyber attacks to express dissent, disrupt operations, or promote an ideology.
    - This may include hacktivism and politically motivated data breaches.
- **Espionage** involves using cyber means to gather secret information, often for military or economic advantages.
    - It can be conducted by both state and non-state actors.

4) Cybercrime Ecosystem

- The **Dark Web** provides anonymity to cyber criminals and facilitates the trade of illicit goods, services, and data.
    - It is a hidden part of the internet, used for illegal activities.
- **Cryptocurrencies** are often used in cyber crime for payments, as they provide anonymity and are difficult to track.
    - Bitcoin and other digital currencies enable anonymous transactions.
- **Roles in facilitating cybercrime:** The dark web and cryptocurrencies enable cybercriminals to operate anonymously, trade illicit goods, and launder money.
    - These tools are crucial for cyber criminals to operate effectively.

5) Role of social media and messaging platforms.

- **Social media** is used by cyber criminals to spread propaganda, recruit members, and conduct phishing attacks.
    - These platforms can be used to spread misinformation and commit fraud.
- **Messaging platforms** are used for encrypted communication between cyber criminals, coordinating attacks and exchanging data.
    - Encrypted messaging apps provide privacy for illegal communications.
- **Social engineering** and phishing attacks exploit vulnerabilities on social media and messaging platforms to steal information.
    - Cyber criminals target users with deceptive practices to gain access to sensitive data.

Data Security & Privacy

1) Importance of Data Security: Why is data protection crucial?

- Data protection is crucial because it **safeguards personal information** from unauthorized access, misuse, and theft.
    - This includes financial, health, and other sensitive information.
- **It ensures business continuity** by protecting company data, avoiding operational disruptions, and preserving trust of customers.
    - Data loss can lead to significant financial and reputational damages.
- Data security is essential for maintaining **economic stability** by preventing financial fraud, and cyber-attacks.
    - Cyber incidents can cause significant financial losses for organizations.
- It **protects national security** by securing critical infrastructure, government data and communications from cyber threats.
    - Cyber attacks can disrupt military operations, and essential services.

- Data protection is crucial for **maintaining public trust** and confidence in government and other organizations.
    - Data breaches and privacy violations erode trust of the public.
- It is necessary for **upholding individual rights** to privacy, as recognized by the Supreme Court.
    - The K.S. Puttaswamy case established privacy as a fundamental right.
- Data security **prevents identity theft**, where personal data is used for fraudulent purposes.
    - This can lead to significant financial and personal harm for individuals.

2) Data Privacy vs Data Security: Understanding the difference.

- **Data privacy** focuses on the appropriate use of personal information, and the rights of individuals over their data.
    - It governs how data is collected, stored, used, and shared.
- **Data security** focuses on protecting data from unauthorized access, theft, or misuse.
    - It involves implementing technological and organizational measures to protect data.
- **Privacy** is about setting boundaries and limiting access to data, while **security** is about protecting data from harm.
    - Privacy ensures that data is used properly, while security ensures its protection.
- **Privacy is a right,** while **security** is a method to ensure the right is protected.
    - Data security is essential to achieve data privacy.
- **Data privacy is a broader concept** that includes data security as a component.
    - Both concepts are interrelated, but not identical.
- **Data security** aims to prevent breaches, while **data privacy** aims to ensure proper handling of data.
    - Both are essential for a secure and trustworthy digital environment.
- The **Digital Personal Data Protection Act, 2023** focuses on ensuring both data privacy and data security.
    - The Act establishes a Data Protection Authority to enforce data protection laws.

Information Technology Act, 2000

- The Information Technology Act, 2000 (**IT Act 2000**) provides legal recognition for transactions via electronic data interchange and other electronic means.
    - It also aims to facilitate e-commerce and deal with cybercrimes.
- The act extends to the whole of India and applies to offenses committed outside India by any person.

Amendments to the IT Act

- The **IT Act was amended in 2008** to exempt intermediaries from liability for third-party information, among other things.
    - This amendment also included new definitions of cyber security, and the establishment of the Indian Computer Emergency Response Team (CERT-In).
- Amendments in 2008 also introduced **Section 66F**, which deals with cyber terrorism.
    - This includes denial of access, unauthorized access, and introduction of contaminants to cause harm to infrastructure.

Important Sections of the IT Act

- **Section 43A** addresses compensation for failure to protect data.
    - It states that a body corporate is liable to pay damages if negligent in implementing reasonable security practices.
- **Section 66** deals with computer-related offenses, including hacking, data theft, and virus introduction.
    - This section outlines penalties for these offenses.
- **Section 66F** specifically addresses **cyber terrorism**, with punishments that may extend to lifetime imprisonment.
    - This section covers offenses that threaten the unity, integrity, sovereignty, or security of the country.

- **Section 69** and **69A** cover the power to issue directions for interception, monitoring, or decryption of information and blocking of websites.
    - These sections are relevant for national security and cyber security.
- **Section 70** deals with protected systems and **critical information infrastructure**.
    - The appropriate government can declare any computer resource affecting critical infrastructure as a protected system.
- **Section 79** provides **exemption from liability for intermediaries** in certain cases.
    - This is subject to due diligence requirements specified in the IT (Intermediary Guidelines) Rules, 2011.

Powers and Functions Under the IT Act

- The Act empowers the **Central Government to make rules** for electronic signatures.
    - This includes specifying the form, content, and security procedures for electronic signature certificates.
- The Act establishes a **Controller of Certifying Authorities** who oversees the issuance and regulation of electronic signature certificates.
    - The controller has the power to grant or reject licenses and investigate contraventions.
- The Act allows for the constitution of a **Cyber Regulations Advisory Committee** to advise the government on matters related to the Act.
    - This committee provides expertise on rules, regulations, and other matters of IT law.
- The Act also gives the government powers to **block websites**.
    - This action is for reasons related to national security or public order.

Working Mechanism of the IT Act

- The IT Act provides a **legal framework for e-commerce and digital transactions**.
    - It gives legal recognition to electronic documents and signatures.
- The Act established **CERT-In** as the national agency for incident response.
    - CERT-In is responsible for responding to computer security incidents, reporting vulnerabilities, and promoting effective IT security practices.
- The Act also provides for an **Appellate Tribunal**, though its composition has been revised.
    - This tribunal exercises jurisdiction and powers conferred by the Act.
- The Act includes provisions for **penalties and compensation** for damage to computer systems and data.
    - These penalties aim to deter cybercrime and compensate victims.
- **Intermediaries have a due diligence** requirement for claiming exemption under Section 79.
    - This includes taking down illegal content after being notified.
- The Act also addresses **data security** through provisions for protecting information, equipment, and devices.
    - This includes implementing reasonable security practices.
- The Act was **amended to include the definition of 'cyber security'** .
    - It means protecting information, devices, and resources from unauthorized access or destruction.

Limitations of the IT Act

- The IT Act **does not adequately address spam**.
    - The word “spam” is not even mentioned anywhere in the IT Amendment Act.
- The Act has **jurisdictional issues** as cyber threats are mostly transnational.
    - It lacks provisions for enabling Indian authorities to assume jurisdiction over data impacting India.
- The Act does not adequately regulate **cryptocurrency**.
- The act has been criticized for not adequately addressing issues related to **confidential corporate information**.
- The maximum compensation stipulated by the act is **only 5 crore rupees**, which is a small figure.
- The IT Act is considered to be **obsolete**.

Digital Personal Data Protection Act, 2023

- The Digital Personal Data Protection Act, 2023 (**DPDP Act 2023**) provides for processing digital personal data while recognizing individuals' rights to protect their personal data and the need to process it for lawful purposes.
- It applies to the processing of digital personal data within India, whether the data is collected digitally or non-digitally and then digitized.
- The act also applies to processing of digital data outside of India if it is related to offering of goods or services to Data Principals within India.

Key Definitions in the DPDP Act

- **Personal data** is defined as any data about an individual who is identifiable.
- **Data Fiduciary** refers to any person, company, or government entity that processes data.
- **Data Principal** is the individual to whom the data relates.
- **Data Processor** processes data on behalf of a Data Fiduciary.
- **Significant Data Fiduciary** has additional obligations based on factors like data volume and sensitivity, and potential impacts.
- **Personal Data Breach** means unauthorized processing, accidental disclosure, or loss of access to personal data that compromises its confidentiality, integrity, or availability.

The Digital Personal Data Protection (DPDP) Act is a law designed to protect your personal data and ensure it is used responsibly. Here's a simplified explanation of its main features:

1. **Key Principles**:
    - The law is based on 7 main rules to handle your data:
        - **Consent**: Your data can only be used if you agree to it.
        - **Lawful Use**: Your data must be used for legal purposes only.
        - **Transparency**: You should always know how your data is being used.
        - **Purpose Limitation**: Data should only be used for specific reasons.
        - **Data Minimization**: Only the data that is absolutely necessary should be collected.
        - **Accuracy**: Your data should be kept correct and up-to-date.
        - **Security**: Strong safeguards should protect your data from misuse.
        - **Accountability**: Those handling your data must take responsibility for its protection.
2. **Consent for Using Data**:
    - Before anyone uses your personal information, they must get your clear and specific permission. This permission must be:
        - **Free**: Given without any pressure.
        - **Informed**: You know exactly what you are agreeing to.
        - **Unconditional**: Not tied to other things.
        - **Clear**: You understand it fully.
3. **Notification**:
    - Before or while collecting your data, you must be informed about:
        - What data is being collected.
        - Why it is being collected and how it will be used.
4. **Your Rights**:
    - You have certain rights regarding your data, such as:
        - **Access**: To know what data is being held about you.
        - **Correction**: To fix errors in your data.
        - **Erasure**: To have your data deleted if it's no longer needed.
        - **Complaint**: To raise issues if you feel your data is being mishandled.
5. **Data Protection Board of India (DPBI)**:
    - A special body, called the DPBI, will ensure everyone follows the law.
    - It will:
        - Handle complaints and grievances.
        - Penalize those who break the law.

Obligations of Data Fiduciaries

- Data Fiduciaries must process data for **lawful purposes**.

    - A lawful purpose is defined as any purpose not expressly forbidden by law.
- They must implement **reasonable security safeguards** to prevent data breaches.
- In case of a **data breach**, Data Fiduciaries must inform both the DPBI and the affected Data Principals.
- They need to establish an **effective grievance redressal mechanism** for Data Principals.
- **Significant Data Fiduciaries** have additional obligations, including appointing a Data Protection Officer, an independent data auditor, and undertaking periodic Data Protection Impact Assessments.

Rights of Data Principals

- Data Principals have the **right to access** information about their personal data.
    - This includes knowing what data is being processed and with whom it is shared.
- They have the **right to correction and erasure** of their personal data.
    - This is applicable when consent was previously given by them.
- They have the **right to grievance redressal** through the Data Fiduciary, and DPBI.
- Data Principals must **not impersonate** anyone, **suppress information**, or register **false complaints**.

Special Provisions

- The Central Government can **restrict data transfers** to specific countries outside India.
- Certain exemptions are provided for processing data in the interest of national security and prevention of crimes.
- The Act stipulates that data fiduciaries cannot process data in a way that has a **detrimental effect on a child**.
    - There is however no clear definition for what constitutes a detrimental effect.

Amendments to other Acts

- The Act has amended the **Information Technology Act, 2000** by omitting section 43A which mandated compensation for mishandling of data.
- It also amended the **Right to Information Act, 2005** to exempt personal information from disclosure.
- The DPDP Act also amends the **Telecom Regulatory Authority of India Act, 1997**.

Powers and Functions of the Data Protection Board of India (DPBI)

- The DPBI is responsible for monitoring compliance with the Act, and **imposing penalties**.
- It can direct **remedial measures** in the event of a personal data breach.
- It will inquire into **breaches and impose penalties** based on complaints by Data Principals.
- The Board will inquire into **breaches by Consent Managers** and intermediaries.

Working Mechanism of the DPDP Act

- The Act establishes a framework for **data processing based on consent**, notice, and specific use.
- It ensures **accountability** through obligations on Data Fiduciaries and remedies for Data Principals.
- The DPBI is the **enforcement authority** for the Act, ensuring compliance and taking action against violations.
- The Act provides for **financial penalties** for breaches of the Act, with penalties up to ₹250 crore for the most serious breaches.
    - The penalties also range from ₹10,000 for breaches of duty by Data Principals, and ₹50 crore for other breaches.
- The act also provides for an **Appellate Tribunal** to hear appeals of the Data Protection Board of India.

Limitations of the DPDP Act

- The act allows **exemptions for the State** which may lead to data collection, processing, and retention beyond what is necessary, violating the right to privacy.
- The act allows for the **transfer of personal data outside India**, which may not ensure adequate protection.
- The act has **removed Section 43A** of the IT Act, which mandated compensation to users for mishandling of data.

- The grievance redressal mechanism requires the individual to first approach the **data fiduciary**, and then the DPBI, before further appeals to the TDSAT.
- The act exempts the **personal information of public officials** from being disclosed under the Right to Information Act, which could aid corrupt practices.

Cyber Security: Data Security & Privacy

1) International Regulations (e.g., GDPR)

- **General Data Protection Regulation (GDPR)** is a regulation in EU law on data protection and privacy. It applies to all organizations that process personal data of EU citizens.
    - GDPR aims to give control to individuals over their personal data and simplifies the regulatory environment.
- **The Budapest Convention** is an international treaty addressing internet and computer crime. It harmonizes national laws and improves international cooperation.
    - India has not joined the convention due to concerns it could infringe on national sovereignty.
- **The Council of Europe Convention (1990)** establishes a common framework for money laundering.
    - It facilitates international cooperation in areas of assistance, search, seizure, and confiscation.
- **International Organization of Securities Commissions (IOSCO)** advises its members to adopt measures to combat money laundering.
    - It addresses measures to combat money laundering in the securities and futures markets.
- **The Financial Action Task Force (FATF)** is an inter-governmental body promoting legal, regulatory, and operational measures to combat money laundering, terror financing, and other threats to the international financial system.
    - It has formulated a series of recommendations that have become international standards.
- **The United Nations Global Programme Against Money Laundering (GPML)** was founded to increase the effectiveness of combating money laundering.
    - It provides complete technical cooperation services to governments.

2) Data Localization: Benefits, drawbacks, and implications.

- **Data localization** refers to the practice of storing data within the geographical boundaries of a country.
    - It mandates that crucial personal data of Indian nationals be processed in Indian-controlled centers.
- **Benefits of Data Localization:**
    - It ensures better **data security and privacy** of Indian citizens, as data is stored locally.
    - It enables **easier access for law enforcement** to investigate crimes and breaches.
    - It can potentially **increase economic activity** by boosting local data centers and infrastructure.
- **Drawbacks of Data Localization:**
    - **Increased costs and complexities** for businesses that have to maintain separate data centers.
    - **Fragmenting of the internet**, creating barriers to data flow and innovation.
    - **Difficulties in cross border data transfer**, impacting services and operations of international companies.
- **Implications of Data Localization:**
    - It could lead to **retaliation from other countries**, leading to a fragmented digital environment.
    - It could result in **increased burden on smaller firms** that have to comply to local data laws.

- The Digital Personal Data Protection Act, 2023, allows for the **transfer of data outside India**, but government can restrict data transfers to specific countries.
    - The Act stipulates that data fiduciaries cannot process data in a way that has a **detrimental effect on a child**.
- **Data storage measures** under the Data Protection Law include the need for a copy of personal data to be kept in India.
    - This is irrespective of where the data is processed.

3) Challenges: How are the data of citizens and government institutions compromised?

- **Cyber attacks** are increasingly common, including hacking, malware injections, and phishing.
    - These attacks can result in data breaches, financial losses, and reputational damage.
- **Cyber warfare** is a growing threat, with state-sponsored actors targeting critical infrastructure.
    - Cyber warfare is considered by some to be a larger threat than terrorism.
- **Cyber terrorism** involves unlawful attacks against computers, networks and information to intimidate or coerce a government.
    - It has become a major threat due to increased convergence of terrorism and cyberspace.
- **Non-state actors** also misuse the internet and social media for subversive activities.
    - This includes the spread of propaganda, recruitment, and coordination of terror activities.
- **Lack of awareness** among users about digital security issues makes them vulnerable to cybercrime.
    - Many people are unaware of the risks and ways to protect their data.
- **Insufficient cybersecurity measures** can compromise data security in both government and private sectors.
    - This is mainly due to outdated security protocols.
- **Pegasus** is a spyware used to remotely surveil mobile phones to boost national security.
    - This technology is sometimes exploited by government and agencies for political reasons.
- **Phishing attacks**, through fraudulent emails, attempt to obtain victims' financial and personal data.
    - These attacks can lead to severe financial losses and data theft.
- **Ransomware** attacks, a type of cyber extortion, can cripple institutions by encrypting and holding their data hostage.
    - This can lead to a complete loss of the victim's private and public trust.
- **The Digital India Program's** success has increased risks associated with cyber-attacks.
    - The increased use of technology means more attack vectors.
- **Cross border cyber-attacks** can lead to the compromise of personal information and critical infrastructure.
    - These attacks can impact the integrity, confidentiality, and availability of information.
- **Data breaches** can lead to identity theft and financial fraud.
    - Data breaches can cause massive losses and erode public confidence.
- **Cloud hosting** of servers may bring cost efficiencies but also poses security risks if not properly managed.
    - There are both advantages and security implications of cloud hosting for government business.
- The IT Act and National Cyber Security Policy of 2013, are considered **outdated** and not well equipped to deal with cybercrimes.
    - The government is working on a new cyber security policy.
- **Social media** is used to spread misinformation and propaganda, impacting social harmony and national security.

    - Social media can be a vehicle for radicalization, recruitment, and terror financing.

National Cyber Security Policy & Framework (India)

1) Key Elements: Goals, initiatives, and approach of the policy.

- The **National Cyber Security Policy (NCSP) 2013** aims to protect public and private infrastructure from cyber attacks.
    - It seeks to safeguard personal, financial, and sovereign data.
- The policy focuses on creating a **secure cyber ecosystem** and building trust in IT systems.
    - It promotes the use of IT in all sectors of the economy.
- The policy emphasizes the need for **indigenous security technologies** and global cooperation.
    - It calls for enhanced research and development.
- The **Cyber Surakshit Bharat Initiative** was launched in 2018 to raise awareness about cybercrime.
    - It builds capacity for safety measures for government IT staff.
- The **Cyber Crisis Management Plan (CCMP)** aims at countering cyber threats and cyber terrorism.
    - It focuses on establishing protocols to respond to cyber incidents effectively.
- The **National Cyber Security Strategy 2020**, conceptualized by DSCI, focuses on 21 areas for a safe cyberspace.
    - It recommends allocating a minimum of 0.25% of the annual budget for cyber security.
        - which can be raised upto 1% has been recommended to be set aside for cyber security.
- The policy includes measures for **securing e-governance services** and protecting critical infrastructure.
    - It encourages the use of open standards.
- The policy calls for an **assurance framework** for the design of security policies.
    - It encourages promotion of global security standards and best practices.

2) Institutional Structure: Roles of CERT-In, National Cyber Coordination Centre (NCCC), and other agencies.

- **Indian Computer Emergency Response Team (CERT-In)** is the national agency for incident response.
    - It issues guidelines, advisories, and vulnerability notes.
- **CERT-In** is mandated to respond to computer security incidents, vulnerabilities and promote effective IT practices.
    - It is responsible for overseeing the administration of the Information Technology Act 2008.
- **National Cyber Coordination Centre (NCCC)** generates situational awareness of potential cyber threats.
    - It enables timely information sharing for proactive and preventive actions.
- **National Critical Information Infrastructure Protection Centre (NCIIPC)** is the nodal agency for the protection of critical information infrastructure.
    - It is responsible for all measures, including R&D for critical infrastructure protection.
- **National Cyber Security Coordinator (NCSC)** coordinates with different agencies for cyber security.
    - NCSC operates under the National Security Council Secretariat (NSCS).
- **Cyber Swachhta Kendra** provides a platform for users to clean their computers of viruses and malware.
    - It is a Botnet Cleaning and Malware Analysis Centre.
- The **National Security Council (NSC)** is the apex body for national security matters.
    - The Prime Minister heads the NSC.
- The **Strategic Policy Group (SPG)** is a coordination forum.
    - It integrates inputs for national security matters.

- The **National Security Advisory Board (NSAB)** undertakes long term analysis and provides perspectives on national security.

3) Challenges: Implementation gaps, technological limitations, lack of awareness, workforce inadequacies.

- The National Cyber Security Policy **lacks proper implementation**, especially regarding the recruitment of professionals.
    - It suffers from a lack of personnel trained in cyber security.
- There is a **lack of awareness** among users about security issues concerning digital communication.
    - Many people are unaware of the risks and ways to protect their data.
- Existing cyber security policies are considered **outdated** and not well-equipped for advanced cybercrimes.
    - The Information Technology Act and NCSP, 2013, are not sufficient.
- There is a **lack of a national security architecture** to effectively assess and respond to cyber threats.
    - This leads to an insufficient response to cyber attacks.
- The policy focuses mainly on **defensive measures**, with no attention to developing offensive capabilities.
    - There is a need to create a "Digital Armed Force" to deter cybercrimes.
- **Technological limitations** and a lack of investment in R&D hinder cyber security efforts.
    - There is a need for more investment in R&D in areas like AI and big data.
- There is a need for a **layered defense** for a comprehensive cyber security framework.
    - This includes firewalls, intrusion prevention systems, and data loss prevention.
- There is **no defined standard procedure** for terrorist classification, blurring the line between a terrorist and a cyber suspect.
    - This results in a need for better legal architecture to deal with complex cybercrimes.

4) Evaluation: Critically evaluate the effectiveness of India's Cyber security policy.

- The National Cyber Security Policy (NCSP) of 2013 is criticized for **focusing only on defensive capabilities**.
    - It does not address the need to develop offensive capabilities.
- The NCSP suffers from **improper implementation**, especially the recruitment of 5 lakh professionals.
    - This indicates a gap between policy goals and their execution.
- The policy **doesn't fine-tune the balance** between national security and freedom of speech and expression.
    - This creates a tension between security measures and civil liberties.
- There is a **lack of coordination** among various agencies in tackling cyber threats.
    - Multiple departments are responsible, making coordination challenging.
- The cyber security policy is **not well-equipped to handle advanced cybercrimes**.
    - Existing laws and policies need to be updated.
- India has been identified as a **vulnerable country** in terms of cyber security threats.
    - A significant percentage of Indian organizations have suffered losses due to cyber incidents.
- Only a small percentage of Indian organizations are considered ready to tackle cyber attacks.
    - This shows the need for more proactive and preparedness for cyber threats.
- There's a need for a **comprehensive cyber security policy**, emphasizing protection of infrastructure and data.
    - The cyber security architecture needs to be strengthened.
- The policy requires emphasis on **human resource development** and training in cyber security.
    - There is also a need to harness the highly skilled IT workforce.

5) Digital Armed Forces: Need, challenges, and future.

- The increasing cyber threats highlight the need for a **"Digital Armed Force"**.
    - This force would be designed to prevent and counter cybercrimes.
- India **lacks a cyber warfare strategy** and needs to develop the capabilities for offensive operations.
    - This includes developing offensive capabilities to deter and respond to attacks effectively.
- There is a need to develop a cyber security strategy similar to the **nuclear doctrine**.
    - Such a strategy should establish clear guidelines, aims and capabilities for cyber defense.
- Developing a **capable cyber force** requires investment in technology, skilled personnel, and training.
    - It requires focus on R&D in Big data, AI, and quantum resistant communications.
- The **challenge** lies in ensuring that a digital armed force does not encroach on civil liberties.
    - This requires explicit privacy laws to balance security needs.
- There is a need to develop **legal architecture** to deal with the increasingly complex nature of cybercrimes.
    - This will require cooperation with international bodies, treaties and agreements.
- A **layered defense** system is necessary, encompassing firewalls, intrusion detection, and data loss prevention systems.
    - It is critical to integrate security into systems from design phase itself.
- **Training of personnel** in cyber-security and harnessing of the skilled IT workforce is also critical.
    - There is also a need to increase public awareness of cyber security.

6) International collaborations: India's cyber security collaborations with other nations.

- India has **bilateral agreements** with developed nations like the US, Singapore, Israel, and Japan to promote research and information sharing on cyber security.
    - These collaborations facilitate knowledge transfer and sharing of best practices.
- **International cooperation** is essential for tackling cyber threats, as they have no geographical restrictions.
    - This includes information sharing, joint exercises, and coordinated responses.
- India should seek to emulate the **cryptographic standards** set by US's National Institute of Standards and Technology (NIST).
    - NIST has developed tools for handling quantum computer attacks.
- India has not joined the **Budapest Convention** due to concerns about national sovereignty.
    - The convention aims to harmonize national laws and increase cooperation on cybercrime.
- India needs to **coordinate with other countries** to develop a global legal framework on cyber terrorism.
    - This includes creating mechanisms for mutual legal assistance and extradition.
- India should collaborate with international bodies to establish **cyber security norms and standards**.
    - This can help in improving information infrastructure and data security.
- There is a need to promote **exchanges and cooperation** at bilateral, regional, and multilateral levels.
    - This can facilitate better incident response, intelligence sharing and capacity building.
- India can also follow **international best practices** such as the Tallinn Manual related to laws on cybercrimes.
    - This would allow India to stay up to date with international cybercrime laws and protocols.

Cyber Security: Social Media & Security

Threats & Challenges: Misinformation, propaganda, radicalization, data breaches.

- Social media platforms are used for **spreading misinformation and disinformation** to manipulate public perception.
    - **Fake news** can cause social unrest, panic and violence.
- Social media is a tool for **propaganda**, used to promote radical ideologies and incite violence.
    - Terrorist organizations use social media to **recruit new members**.
- Social media facilitates **radicalization** by exposing individuals to extremist content and hate speech.
    - This can lead to the transformation of individuals into **violent extremists**.
- **Data breaches** on social media platforms can expose personal and sensitive information of users.
    - This includes passwords, financial data, health data, and sexual orientation.
- **Cyber warfare** uses the internet to impact strategic or military operations through information warfare.
    - It involves **deliberate assaults on information systems** for strategic or military reasons.
- Social media has a high concentration of online security vulnerabilities, making it prone to attacks.
    - This makes user data and personal information vulnerable to misuse.
- Non-state actors use the internet and social media for **subversive activities**, posing a major security concern.
    - These actors can operate outside the government's control.
- Social media platforms are used for **cyber terrorism**, which includes attacks on computers, networks, and data.
    - These attacks are aimed at intimidating governments or people.

Impact on National Security: Threat to law and order, social harmony, democracy.

- Social media fueled misinformation can **threaten law and order** by inciting violence, riots, and public unrest.
    - **Biased reporting** and fake news can create instability.
- Social media can disrupt **social harmony** by spreading hate speech, religious intolerance, and communal disharmony.
    - Radicalization on social media can lead to **communal violence and distrust**.
- Social media misuse can impact **democracy** by manipulating elections through misinformation campaigns.
    - It can create instability, challenge the authority of the government, and threaten humanity.
- The spread of misinformation through social media can undermine **public trust** in institutions and media.
    - This makes citizens more vulnerable to manipulation.
- Social media platforms can be used by non-state actors to **challenge the authority of the government**.
    - They can create instability by propagating anti-government sentiments.
- **Terrorists** use social media to spread propaganda and recruit new members, thereby threatening national security.
    - This poses challenges to internal security and national stability.
- Social media can be used for **economic sabotage** through the spread of misinformation and propaganda.
    - This can disrupt economic activities and investor confidence.
- Cyber attacks on critical infrastructure facilitated through social media, can **threaten national stability and security**.
    - Attacks on critical infrastructure can disrupt essential services, such as power, communication, etc.

Counter Measures: Government regulations, fact-checking initiatives, social media companies' responsibilities.

- Governments should develop **indigenous counter-radicalization programs** to disseminate a counter narrative.
    - This helps to combat the spread of radical ideologies on social media.
- **Fact-checking initiatives** and awareness campaigns are necessary to debunk misinformation on social media.
    - Users should question sources and check the credibility of content before sharing.
- Social media companies should be held **responsible for monitoring and removing harmful content**.
    - They need to ensure accountability for the content posted on their platforms.
- **Regulations** must be put in place to control the spread of fake news and propaganda.
    - These regulations should not impinge on freedom of speech and expression.
- Governments must enhance **technical surveillance** and intelligence gathering to track and prevent cyber threats.
    - This includes increased monitoring of social media and other online platforms.
- **Specialized task forces** and research wings can be created to tackle cyber threats effectively.
    - These forces should be trained to handle complex cyber attacks and online propaganda.
- **Cyber security standards** should be defined not only for government but also private organizations.
    - Private companies should follow a checklist of requirements to protect their systems and data.
- A **Security Incident Management and Response System** must be established to handle digital security attacks.
    - This includes sectoral Cyber Security Incident Response Teams (CSIRTs).

Ethical Dilemmas: Balancing security with freedom of speech and expression.

- There is a need to **balance security** with freedom of speech and expression, which are both critical.
    - Regulations to control social media must not be excessive and should be within constitutional limits.
- Governmental measures to counter cyber threats must be **transparent and accountable**.
    - Measures should not infringe on civil liberties.
- **Over-regulation** of social media can result in censorship and undermine democratic principles.
    - Excessive control can stifle dissent and public discourse.
- **Surveillance** measures must be used judiciously and ethically, protecting individual privacy.
    - There should be proper oversight and accountability of these measures.
- The **definition of misinformation** should be clear and not be misused to suppress dissent or opposing views.
    - It is necessary to distinguish between misinformation and freedom of expression.
- **Legal frameworks** must balance security needs with the rights of individuals.
    - This ensures legal and judicial oversight of government action.
- The banning of terrorist organizations must be done without infringing on fundamental rights.
    - The provision of designating individuals as terrorist can be misused against political opponents.
- There should be a balance between preventing the misuse of social media and protecting the rights of citizens.
    - This includes the right to information, right to privacy and right to protest.

Role of Artificial Intelligence in tackling social media menace.

- Artificial intelligence (AI) and machine learning (ML) can be used to **identify digital security attacks and breaches**.
    - This helps in the early detection and mitigation of cyber threats.
- AI can be used to **form a database of specific accounts, sources, and IP addresses** linked to fake news.
    - This allows detection mechanisms to identify and flag potential sources of misinformation.
- AI can be used to **analyze and detect patterns** in the spread of misinformation and hate speech.
    - This helps in taking proactive measures to prevent the spread of harmful content.
- AI can help in **automating fact-checking** and identifying fake news with greater efficiency and scale.
    - This enhances the ability to quickly verify content before it goes viral.
- AI can help in the **monitoring and removal of extremist content** on social media platforms.
    - This helps prevent the radicalization of individuals through exposure to harmful content.
- **AI can be used to enhance cyber security** by detecting and blocking malicious software and attacks.
    - This provides better protection for users and networks against cyber threats.
- AI can be used to **predict potential future attacks**, improving the overall security infrastructure.
    - This helps security agencies to prepare for upcoming cyber threats.
- **AI should be used ethically**, ensuring transparency, fairness and accountability in its deployment for security.
    - This safeguards the rights and freedom of individuals while ensuring security.

Cyber Security Framework & Measures

Elements of a Comprehensive Cyber Security Framework: Risk assessment, prevention, detection, response, and recovery.

- A comprehensive framework includes **risk assessment** to identify vulnerabilities and potential threats to systems.
    - This involves evaluating the likelihood and impact of cyber incidents.
- **Prevention** measures are crucial, employing tools to stop cyber attacks before they occur.
    - This includes firewalls and intrusion prevention systems.
- **Detection** capabilities are needed to identify attacks and breaches that have bypassed prevention measures.
    - This requires continuous monitoring and analysis of network traffic.
- **Response** involves a plan of action during a cyber attack to minimize damage and restore services.
    - A **Cyber Crisis Management Plan (CCMP)** should be in place to counter threats.
- **Recovery** focuses on restoring systems and data after a cyber attack while improving security.
    - This should include offline backups and system restoration.
- A layered defense is needed for a comprehensive framework, with multiple layers for protection.
    - This includes firewalls, data loss prevention and antivirus software.
- The framework should include **security standards** for government and private companies.
    - These standards should be enforced with a checklist of requirements.
- The framework must provide for **continuous monitoring** and assessment to ensure security.
    - This helps in the early detection and mitigation of vulnerabilities.

Defensive Measures: Firewalls, intrusion detection systems, encryption, security audits, patch management.

- **Firewalls** are essential for network security, filtering traffic and blocking unauthorized access to systems.
    - They act as a barrier between a trusted network and untrusted external networks.
- **Intrusion detection systems (IDS)** monitor networks for malicious activity and alert security personnel.
    - These systems help in detecting attacks and preventing potential breaches.
- **Encryption** is crucial for protecting sensitive data by converting it into unreadable code.
    - It ensures that only authorized parties can access and decipher data.
- **Security audits** regularly assess the security posture of systems and identify potential vulnerabilities.
    - They help in identifying and remediating weaknesses in security protocols.
- **Patch management** involves updating software and systems to fix security vulnerabilities.
    - This prevents hackers from exploiting known bugs in systems and software.
- **Demilitarized zones (DMZ)** add a layer of security between public and internal networks.
    - This helps protect the internal network from direct exposure to threats.
- **Data loss prevention (DLP)** measures are used to prevent sensitive data from being exfiltrated.
    - These measures include tools that monitor and prevent the transfer of confidential data.
- Implementing **minimum security specifications** for all systems is vital for cyber defense.
    - This helps ensure that all systems meet basic security standards.

Incident Response: What to do during a cyber attack.

- A well-defined incident response plan is crucial to **minimize the impact of a cyber attack**.
    - This should outline roles, responsibilities and actions.
- **Isolating** affected systems is important to prevent the spread of an attack to other parts of the network.
    - This contains the damage caused by the cyber incident.
- **Identifying the source** and nature of the attack is necessary to take appropriate action.
    - This includes analyzing network traffic and system logs to determine the source.
- **Eradicating** the malware or attack vector should be done as quickly as possible.
    - This stops the attack from continuing or recurring.
- **Recovering** systems and data from backups can help to restore services with minimal disruption.
    - This ensures business continuity after a cyber attack.
- **Reporting incidents** to the appropriate authorities is necessary for coordination and future prevention.
    - This helps other organizations in the sector to be aware of the threat.
- **Documenting every step** of the incident response is important for learning and future preparation.
    - This also helps with any investigation and legal proceedings that may follow.
- **Post-incident review** is needed to understand the lessons learned and improve the incident response plan.
    - This should be done to prevent future attacks by improving security measures.

Cyber hygiene: What is cyber hygiene and how can we promote cyber safety at individual level.

- **Cyber hygiene** includes practices and habits individuals use to maintain their digital safety and security.
    - It aims at protecting devices and networks from cyber threats.
- Users should **use strong, unique passwords** for their accounts and change them regularly.
    - This reduces the risk of password theft and unauthorized access.
- It's crucial to **enable multi-factor authentication (MFA)** to provide an extra layer of security for accounts.
    - This requires multiple verification methods for accessing a user account.

- Users should be cautious about **phishing attempts** and avoid clicking on suspicious links or attachments.
    - This prevents users from revealing personal information to hackers.
- Keeping software and operating systems **updated** is vital to patch security vulnerabilities.
    - This helps prevent malware from exploiting vulnerabilities.
- **Being careful about sharing information** online, can help prevent personal data from being exposed.
    - This includes being cautious about social media profiles and activities.
- Using **reputable antivirus software** on computers and devices is necessary to detect and remove malware.
    - This helps to defend against viruses, trojans and other harmful software.
- **Increasing awareness** among users about security issues is essential for promoting cyber safety.
    - This can be done through various awareness programs and campaigns.

Role of Technology: How new technologies like AI, ML, Blockchain, Cloud can help in combating cyber threats.

- **Artificial Intelligence (AI) and Machine Learning (ML)** can help in identifying complex cyber attacks.
    - AI and ML can be used to detect patterns and anomalies that may indicate a cyber attack.
- AI and ML can enhance **threat detection** and response capabilities by automating security processes.
    - These technologies can help with intrusion detection and malware analysis.
- **Blockchain** technology can provide secure and transparent transactions and data storage.
    - It can be used to secure data and prevent unauthorized access.
- **Cloud computing** offers scalable and flexible security solutions for data storage and management.
    - It allows for centralized security controls and efficient threat management.
- **AI can help in automating fact-checking** and identifying fake news with greater efficiency.
    - This can help in verifying content and preventing the spread of misinformation on social media.
- **Quantum-resistant communications** are necessary for protecting critical sectors from quantum computer attacks.
    - Developing capabilities in this field is essential for future security.
- **Edge computing** allows for data processing closer to the source, reducing latency and increasing security.
    - This can enhance the responsiveness and efficiency of cyber security measures.
- **Big Data analytics** can be used to process and analyze large amounts of data to identify cyber threats.
    - This helps to improve threat detection and prevention capabilities.

IoT Security: Vulnerabilities and implications of interconnected devices.

- **IoT devices often lack basic security features**, making them vulnerable to attacks. These devices may rely on default passwords that give attackers easy access.
- **Many IoT devices lack human users who can install security updates**, making it difficult to patch vulnerabilities.
- The **interconnectedness** of IoT devices creates more entry points for cyber threats.
- **Compromised IoT devices can form botnets** that can be used for volumetric attacks, data theft, or brute force attacks.
- The **lack of universal security standards** requires unique approaches to manage authentication and access for each implementation.

Cloud Security: Challenges and solutions for securing cloud infrastructure.

- **Centralized cloud computing architecture** is vulnerable to distributed denial-of-service (DDoS) attacks and power outages.
- **Cloud infrastructure** can be exploited due to weak security measures, leading to damaging breaches.
- **Data stored on a cloud provider's server** can be viewed by a firm employee, and the data owner might have limited control over personnel.
- **Cloud security solutions** should offer scalable and flexible security for data storage and management.
- The **National Cloud of NIC** hosts products for website generation and deployment using secure templates.
- **Cloud services** must adhere to security compliance under the IT Act of 2000.
- **Cyber Swachchta Kendra (CSK)** is a dedicated cloud for digitizing and automating processes for the Indian Army, similar to the national cloud initiative, Meghraj.

Blockchain: How can it improve security?

- **Blockchain technology** provides secure and transparent transactions and data storage.
- **It can be used to secure data** and prevent unauthorized access by using cryptographic techniques.
- **Blockchain's distributed nature** makes it resistant to single points of failure and tampering.
- The **use of blockchain** can enhance data integrity through its immutable nature.

Quantum Computing and Cyber Security: How is it a game changer and potential threat?

- **Quantum computing** poses a significant threat to current cryptographic systems.
- **Quantum computers** can potentially breach hardened targets and expose digital infrastructure.
- **Quantum-resistant communications** are necessary to protect critical sectors from quantum computer attacks.
- India must develop capabilities in **quantum-resistant cryptography**.
- **Quantum technology** can be used for better prediction and identification of digital security attacks.
- **Research and development** in quantum technology is critical for cyber security.

Money Laundering and its Prevention 1
Money Laundering and its Prevention 1
Money Laundering and its Prevention: Core Concepts 1
1) Definition: Money Laundering, Black Money, Parallel Economy 1
Sub-Points and Details: 1
2) Stages of Money Laundering: Placement, Layering, Integration 1
Sub-Points and Details: 2
3) Linkages: Money laundering's connection with other illicit activities (drug trafficking, gunrunning, human trafficking) 2
Sub-Points and Details: 2
Causes: Why money laundering occurs 3
Economic Effects: Impacts on the Indian economy and stability 4
National Level Measures: 5
Prevention of Money Laundering Act (PMLA) and its key features 5
Important sections of the Prevention of Money Laundering Act (PMLA) include: 6
National Level Measures 7
1) Enforcement Agencies 7
2) Demonetisation & its impact on parallel economy 8
3) Digitalisation of transactions & their implications 8
4) Role of Banking Sector and Other Financial Institutions 8
5) KYC Norms and Their Significance 8
International Level Measures 9
1) FATF (Financial Action Task Force) and its Role 9
2) International Cooperation and Treaties 9
3) Role of Interpol and Other International Agencies 10
4) Information Sharing Mechanisms 10
Emerging Challenges & Trends 10
1) Technological Advancements (Crypto-currencies, Online Gambling) 10
2) Globalization and its Impact 11
3) Use of Shell Companies and Tax Havens 11
4) Political Factors/Corruption 11
Case Studies (Indian & Global) 11
1) Real-world Examples of Money Laundering Cases (e.g., specific scams or instances). 11
2) How Different Countries Have Tackled Money Laundering 12

Money Laundering and its Prevention

- [ ] (84/20): Recall the important measures undertaken by the Government to reduce the operations of the parallel economy in India. Do you think these measures have been effective?
- [ ] (GS 2, 85/20): What is black money and why is it so called? Specify the main causes of its generation in India.
- [ ] (87/3): The economic offenders often thrive in a parallel economy. Is it true or false? Explain your view.
- [ ] (GS 2, 00/15): Discuss the economic effects of Black money (Parallel economy) in the Indian economy.
- [ ] (00/3): What do you mean by 'Parallel Economy'?
- [ ] (13/10): Money laundering poses a serious security threat to a country's economic sovereignty. What is its significance for India and what steps are required to be taken to control this menace? (200 words)
- [ ] (2018, 15 Marks): India's proximity to two of the world's biggest illicit opium-growing states has enhanced her internal security concerns. Explain the linkages between drug trafficking and other illicit activities such as gunrunning, money laundering and human trafficking. What countermeasures should be taken to prevent the same? (250 words)
- [ ] (2021/10): Discuss how emerging technologies and globalisation contribute to money laundering. Elaborate measures to tackle the problem of money laundering both at national and international levels.

Money Laundering and its Prevention

Money Laundering and its Prevention: Core Concepts

1) Definition: Money Laundering, Black Money, Parallel Economy

- **Money laundering** hides illegal income sources via complex transactions.
    - It cleans illegitimate money, making it appear legal.
- **Black money** is income hidden from tax authorities.
    - It comes from unreported legal and illegal activity.
- The **parallel economy** is an economic system that operates outside of formal economy
    - It is also referred to as black, illegal or unaccounted economy.

Sub-Points and Details:

- Money laundering involves **placement, layering, and integration**.
    - Placement is the introduction of dirty money into the financial system.
- Layering conceals the source of the money through various transactions.
- Integration involves using the money for legitimate purposes.
- **The Prevention of Money Laundering Act of 2002 (PMLA)** defines money laundering as any activity connected with proceeds of crime.
    - This definition includes concealing, possessing, acquiring, or using proceeds of crime.
- **Black money** creation includes manipulation of IPOs, shell companies, and public procurement.
- **Hawala** is an informal, low-cost technique to transfer money without banks or other institutions.
    - It relies on codes and contacts instead of formal documentation.
- **The Financial Action Task Force (FATF)** has defined money laundering as “the practice of hiding unlawful income from derived from criminal activities”.
- **Global Money Laundering** is estimated to be between 2 and 5% of the world’s GDP.
- **The Criminal Law Amendment Ordinance** covers proceeds from corruption, breach of trust, and cheating.
    - However, it does not cover all offences under the Indian Penal Code.
- **The Smugglers and Foreign Exchange Manipulators Act** deals with property acquired through smuggling and foreign exchange manipulation.

2) Stages of Money Laundering: Placement, Layering, Integration

- **Placement** introduces "dirty" money into the legitimate financial system.
    - This is the first stage where the money enters the system.
- **Layering** conceals the source of the money via multiple complex transactions.
    - This involves a series of transfers to obscure the original source.
- **Integration** is when the laundered money is used for legitimate purposes.
    - At this stage, the money appears to be clean and from a legal source.

Sub-Points and Details:

- Placement methods include structuring, bulk cash smuggling, and cash-intensive industries.
    - It also involves the use of shell companies and round-tripping.
- Layering uses techniques like shell companies, and structuring transactions.
    - It also involves transferring money through various accounts and locations.
- The use of **shell companies** in layering helps to hide the source of funds.
- Integration includes investments in real estate, businesses, or luxury assets.
    - The money is integrated into the formal economy.
- **Hawala** is a system used in the layering stage to transfer money informally.

    - It operates outside of traditional banking systems.
- **Structuring** involves breaking large amounts of cash into smaller deposits to avoid reporting requirements.
    - This method is also known as "smurfing".
- **Credit cards** are used to launder money across borders.
    - They can be used to make purchases that are then resold.
- **Emerging technologies** and **globalization** contribute to money laundering.
    - Faster transmission and concealment of the source are facilitated by technology.
- **Cryptocurrency** can be used in money laundering activities.
- **The Financial Action Task Force (FATF)** has defined money laundering as “the practice of hiding unlawful income from derived from criminal activities”.

3) Linkages: Money laundering's connection with other illicit activities (drug trafficking, gunrunning, human trafficking)

- **Money laundering** is intrinsically linked to various criminal activities.
    - It provides the financial means to sustain illicit operations.
- Drug trafficking is a major source of funds for money laundering activities.
    - **Narcotics trade** is systematically used to fund terrorist and underworld groups
- **Gunrunning** and money laundering are also closely connected.
    - Both activities require logistical assistance and financial resources.
- **Human trafficking** is another source of illegal funds that are laundered.
    - Smuggling of narcotics is often intertwined with human trafficking.

Sub-Points and Details:

- **Terrorist networks** are often funded by black money obtained through drug trafficking.
    - This money is then used to support their operations.
- **Illicit activities** like illegal arms sales, smuggling, drug and prostitution generate huge amounts of proceeds.
    - These proceeds are then laundered to make them appear legitimate.
- The **Golden Crescent** (Afghanistan) and **Golden Triangle** (Myanmar) are primary opium-producing regions.
- These regions contribute significantly to the illegal drug trade and related money laundering.
- **Organized crime** is another major activity associated with money laundering.
    - Criminal networks use money laundering to conceal their profits.
- **Counterfeit currency** corrodes the economy, it also facilitates black money and money laundering.
- **India's proximity** to major opium-growing states enhances internal security concerns
    - This proximity links drug trafficking with other illicit activities.
- The **Taliban** uses the proceeds from the drug trade for various purposes including weapons
- **Illegal wildlife trade** is also linked to money laundering.
- **Cyber enabled fraud** is one of the main sources of money laundering

Causes: Why money laundering occurs

- Money laundering hides the illegal source of income by complex transfers.
    - It "cleans" illegitimate money making it appear legal.
- Money is laundered to evade taxes and hide wealth from authorities.
    - Tax havens with secrecy allow financial transactions.
- Corruption is a major source of money for laundering, increasing illegal activities.
    - Black money is kept hidden from tax officials.
- Organized crime, drug trafficking, and illegal arms sales generate laundered funds.
    - Criminal activities generate money which is not reported to authorities.
    - Narcotics trafficking and smuggling fund terrorist networks.
- Money laundering is facilitated by both emerging technologies and globalization.
    - Digital technologies provide new ways to launder money.

- Money laundering undermines economic stability, integrity of financial markets.
    - It distorts economic policy and increases instability.
- Hawala is an informal system that facilitates money laundering.
    - It transfers money without using banks or formal institutions.
- Cryptocurrencies enable money laundering.
    - These transactions are often difficult to trace.
- Illegal wildlife trade is connected to money laundering.
    - This illicit activity helps generate and move illicit funds.
- Money laundering is a process to integrate "dirty money" into financial systems.
    - Placement, layering and integration are three process steps.
- Non-profit organizations are sometimes used to launder money.
    - Tax rules for these organizations are abused.
- Shell companies are used in laundering, facilitating transactions without real business activities.
    - Fake invoices and balance sheets are used by these companies.
- Structuring deposits in smaller amounts avoids anti-money laundering reporting.
    - This is sometimes referred to as "smurfing".
- Credit cards and third party accounts are used to launder money.
    - These instruments often have multiple uses across borders.
- Trade-based money laundering uses disguising of proceeds through trade
    - It attempts to legitimize illicit money flows.
- The primary sources of money laundering in India are cyber-enabled fraud, corruption, and drug trafficking.
    - These are all illegal activities committed within the country.
- Terror financing and organized crime are also increasingly involved.
    - This includes human trafficking and cyber terrorism.
- Money laundering is also used to fund illegal arms and smuggling operations.
    - This leads to further crimes and destabilization.
- Money laundering poses a threat to a country's economic sovereignty.
    - It has a large negative impact on financial systems.
- The process of money laundering conceals the source of the money.
    - It gives an appearance that the money came from legitimate sources.
- Laundered money creates a parallel economy, negatively impacting the main economy.
    - This also helps to create a large informal economic sector.
- The goal of money launderers is to conceal the illegal origin of funds.
    - The process "legitimizes" illegal gains.
- Terrorist groups utilize money obtained from illegal activities like narcotics.
    - Smuggling to fund their activities.
- Real estate transactions, bullion and jewelry purchases, are used for money laundering.
    - These are often disguised to evade taxes.
- Manipulation of initial public offerings (IPOs) and shell companies facilitate money laundering.
    - Public procurement has seen a rise in money laundering.
- Offshore financial centers are also used to launder money.
    - These centers feature financial systems designed to hide assets.
- Loss of revenue occurs due to money laundering which increases government debt.
    - Borrowing increases government debt.
- High real estate prices in major cities is the result of money laundering.
    - These prices create an investment environment for laundered funds.

Economic Effects: Impacts on the Indian economy and stability.

- Money laundering **undermines the legitimacy of the private sector** and financial markets.
    - It reduces trust in the financial system.
- Money laundering **distorts economic policy and creates economic instability**.

    - It can cause unanticipated fluctuations in interest and exchange rates.
- It can **lead to loss of confidence in economic institutions** and increase corruption.
    - This undermines good governance and the rule of law.
- Money laundering **reduces human development** by misallocating resources and eroding morals.
    - It degrades social standing and encourages illicit activities.
- Money laundering **contributes to organized crime and terrorism financing**, which impacts national security.
    - This can also reduce the availability of resources for legitimate uses.
- It can also lead to **loss of useful resources for the nation**.
    - This includes both natural and financial resources.
- Money laundering **increases the level of societal illegality and crime**.
    - This can degrade social cohesion.
- It **creates a parallel economy** that is outside of government oversight and regulation.
    - This can make it more difficult for the government to manage the economy.
- The process of money laundering **conceals the true source of illegally obtained money**.
    - This gives the money a seemingly legitimate origin.
- Money laundering results in the **loss of tax revenue**, which increases government debt.
    - This is a direct cost to the public.
- It **creates an environment of high real estate prices** in major cities, impacting affordability.
    - This is due to money launderers investing in real estate.
- Money laundering **facilitates illicit activities** such as drug trafficking and smuggling.
    - These activities also harm communities and societies.
- It can also result in **instability of the political system** due to criminalization.
    - This is due to the involvement of money laundering in elections.
- The process of money laundering **creates a demand for fake currency**, harming the financial system.
    - This also increases the amount of illegal activity.
- The **transfer of dirty money** through illegitimate channels **hurts legitimate financial channels**.
    - This reduces the capacity of formal systems to allocate capital efficiently.
- Money laundering can lead to the **erosion of public trust in institutions**.
    - It causes a lack of confidence in the integrity of the government.
- Money laundering **creates opportunities for further crimes** by "legitimizing" ill-gotten gains.
    - This also makes it easier to engage in other illegal activities.
- **Terrorist networks are funded by black money** from activities such as drug smuggling.
    - This has a direct impact on national security.
- Money laundering is used in the **financing of illegal arms and smuggling operations**.
    - This increases the level of violence and crime in a society.
- Money laundering can **undermine a country's economic sovereignty**.
    - It leads to a loss of control of the financial system.
- **Global money laundering** is estimated to be **between 2 and 5% of global GDP**.
- This shows the scale of this problem.
- Money laundering **enables tax evasion** and can also **facilitate trade in endangered animals**.
    - It creates a black market for illicit goods.
- **Corruption, cyber-enabled fraud, and drug trafficking** are the primary sources of money laundering in India.
    - These sources highlight the range of illegal activities driving the process.
- Money laundering **increases the gap between the rich and the poor**, due to the illicit nature of the activities.
    - This leads to social and political tensions.

National Level Measures:

Prevention of Money Laundering Act (PMLA) and its key features.

- The **PMLA** was enacted in 2002 to **combat money laundering** and confiscate related property.
    - It addresses both money laundering and its connected activities.
- **PMLA** defines money laundering as any activity connected to proceeds of crime as untainted property.
    - This includes direct or indirect involvement in related processes.
- **PMLA** aims to prevent money laundering and its use in illegal activities.
    - It also seeks to prevent economic crimes.
- The **PMLA** provides for the **confiscation of property** involved in money laundering.
    - This includes property derived from or used in money laundering.
- **Offences under PMLA** include those listed in Parts A and C of the Schedule.
    - Part A lists offences under acts like the Indian Penal Code and the Information Technology Act.
    - Part C deals with trans-border crimes.
    - Part B specifies offenses from Part A with a value of Rs 1 crore or more.
- The **Enforcement Directorate (ED)** is responsible for investigating money laundering offenses.
    - It has the power to seize property if it is proven to be proceeds of a crime.
- The **Financial Intelligence Unit-India (FIU-IND)** receives and analyzes reports of suspicious transactions.
    - It coordinates with national and international intelligence agencies to combat money laundering.
- **PMLA** requires financial institutions to authenticate client identification and maintain records.
    - They must report suspicious financial transactions.
- **The 2019 judgment** in Vijay Madanlal Choudhary vs. Union of India upheld key PMLA provisions.
    - The court emphasized that money laundering is as serious as terrorism.
- **PMLA** was amended to include Politically Exposed Persons (PEPs) and crypto transactions.
    - It also widened the scope of reporting entities to include NGOs.
- The PMLA Act was amended to bring practicing chartered accountants and other professionals under its ambit.
    - These professionals must report financial transactions conducted on behalf of their clients.
- The **PMLA** has a wide reach and captures any activity dealing with proceeds of crime.
    - It is not limited to the final act of integrating tainted property into the formal economy.
- The PMLA allows for the **temporary attachment and forfeiture of property** of those involved in money laundering.
    - This helps to prevent further illegal activities by taking away the ill-gotten gains.
- The court determined that the accused in a money laundering case must prove their innocence. * This places a burden of proof on the accused, not the prosecution.
- **Penalties for financial institutions** involved in laundering include fines and other penalties.
    - The Act was amended to remove the upper limit on fines.
- The **PMLA of 2002** had a provision for a fine of up to Rs 5 lakh, however, the amendment removed this ceiling.
    - This change makes the penalties more effective.

Important sections of the Prevention of Money Laundering Act (PMLA) include:

- **Section 3** defines the offense of money laundering as any process or activity connected with the proceeds of crime, including concealment, possession, acquisition, or use, and projecting it as untainted property. This section has a wide reach, capturing every direct or

indirect process or activity in dealing with the proceeds of crime. The 2019 amendment to Section 3 expanded the scope to include any activity of concealment, possession, or acquisition individually as an offense.

- **Section 4** specifies the punishment for money laundering, which includes rigorous imprisonment for a minimum term of three years, extending up to seven years, and a fine without any limit.
- **Section 5** deals with the attachment of property involved in money laundering. It allows for the seizure or freezing of property, records, and attachment of property obtained with the proceeds of crime.
- **Section 8** discusses the process of adjudication of seized property. The amended Section 8(8) empowers the Special Court to restore confiscated assets to the rightful claimants even during the trial.
- **Section 12** outlines the obligations of banking companies, financial institutions, and intermediaries to maintain records and report suspicious transactions. These entities are required to authenticate the identification of their clients, keep records, and provide information to the Financial Intelligence Unit-India (FIU-IND).
- **Section 17** and **Section 18** deal with search and seizure. Under these sections, an arrest can be made for an offense under the PMLA even without a First Information Report (FIR). These sections are at par with Section 19, where no pre-condition exists to forward a report under Section 157 of the Criminal Procedure Code (CrPC) or to seek warrants from the Court for making an arrest.
- **Section 19** empowers the Enforcement Directorate (ED) to make arrests after recording reasons to do so and forwarding the report to the adjudicating authority.
- **Section 24** outlines the burden of proof, stating that a court will presume an accused to be involved in money laundering unless proven otherwise. This is a reverse burden of proof, in contrast to the common law principle of "innocent until proven guilty".
- **Section 45** imposes two conditions for bail in PMLA cases: first, an opportunity for a prosecutor to oppose the bail, and second, the prima facie satisfaction of a court on the presence of reasonable grounds that the accused is not guilty of money-laundering and that they are not likely to commit any offense while on bail.
- **Section 50** authorizes an ED officer to summon any person to record statements during an investigation.

The Supreme Court of India has made several key rulings regarding the provisions of the Prevention of Money Laundering Act (PMLA), primarily in the case of **Vijay Madanlal Choudhary vs. Union of India**, which upheld many aspects of the PMLA. Here are some of the key rulings:

- **Definition of Money Laundering (Section 3):** The Supreme Court upheld the wide interpretation of Section 3 of PMLA, which defines money laundering. The court ruled that **Section 3 captures every process and activity, direct or indirect, in dealing with the proceeds of crime**, and is not limited to the final act of integrating tainted property into the formal economy. It also interpreted the word "and" in the concerned laws as "or" to give full effect to the legislative intent. The court rejected the argument that mere concealment or possession of the proceeds of crime cannot be considered money laundering; they are indeed a part of the offense.
- **Attachment of Property (Section 5):** The Court upheld the powers of the Enforcement Directorate (ED) regarding provisional attachment and confiscation of properties. It stated that the **registration of a scheduled offense or a formal complaint is not a pre-condition** for resorting to provisional attachment. This ruling allows the ED to make emergency attachments of properties for a period of 180 days without a prior registered criminal case.
- **Search and Seizure (Sections 16, 17, and 18):** The Supreme Court rejected objections to the 2019 amendment that did away with the requirement of informing a court before a search and seizure. The court noted that **searches and seizures under PMLA are not only for inquiring into the offense of money laundering, but also for its prevention**.

- **Power to Arrest (Section 19):** The Court upheld the power of the ED to make arrests under Section 19, emphasizing that the **power to make arrest is essential to achieve the objective of the law**. The court stated that PMLA aims to both prosecute and prevent money laundering, thereby justifying the power of arrest.
- **Summons and Self-Incrimination (Section 50):** The Court rejected the argument that Section 50 of PMLA, which authorizes ED officers to summon any person to record statements, violates Article 20(3) of the Constitution which provides protection against self-incrimination. The court stated that **ED officers are not police officers**, and that statements made to them are admissible as evidence. It also said that if the statement made reveals the offense of money laundering or existence of proceeds of crime, that becomes actionable under the act itself.
- **Reverse Burden of Proof (Sections 24 and 45):** The court upheld the reverse burden of proof in Sections 24 and 45 of PMLA, which means that **a court will presume an accused to be involved in money laundering unless they prove otherwise**. The court stated that, although the presumption of innocence is a human right, it can be interdicted by a parliamentary law. The accused would get enough opportunity before the authority or the court to discharge his burden.
- **Bail Provisions (Section 45):** The Supreme Court upheld the stringent twin conditions for bail under Section 45 of the Act. These conditions require the public prosecutor to have an opportunity to oppose bail and require the court to be satisfied that there are reasonable grounds to believe the accused is not guilty of money laundering and is not likely to commit any offense while on bail. The court noted that money laundering is as serious as terrorism, thereby justifying tough bail conditions.
- **Retrospective application of the offense of money laundering:** The SC upheld that the offense of money laundering is a continuous one, hence it can be acted upon independent of when the scheduled offense was committed. This means holding property derived from an offense which may not have been a scheduled offense at the time of commission will also be defined as money laundering.

These rulings have broadly strengthened the PMLA and the powers of the ED in investigating and prosecuting money laundering offenses.

National Level Measures

1) Enforcement Agencies

- **Enforcement Directorate (ED)** is a law enforcement and economic intelligence agency.
    - It enforces economic laws and combats financial crimes.
    - It investigates money laundering offenses (PMLA).
    - The ED can seize property if proven to be from scheduled offenses.
- **Financial Intelligence Unit-India (FIU-IND)** is an autonomous body.
    - It reports directly to the Finance Ministry's Economic Intelligence Council (EIC).
    - It coordinates and strengthens national and international intelligence efforts.
    - FIU-IND integrates financial organizations within the PMLA's reporting structure.
- **Central Bureau of Investigation (CBI)** is responsible for investigating scheduled offenses.
    - It investigates cases of corruption, fraud, and cheating which may involve money laundering.

2) Demonetisation & its impact on parallel economy

- Demonetisation is when a government removes a form of currency from legal circulation.
    - It aims to curb black money, counterfeit currency and terror financing.
- It can be a tool to reduce the amount of unaccounted for money in the economy.
- Demonetization may cause disruption to the economy during implementation.
- There is a risk of economic disruption, especially in sectors that rely heavily on cash transactions.
- Demonetisation alone is not enough to eradicate the parallel economy.
    - Other measures and reforms are needed to address the root causes of the problem.

3) Digitalisation of transactions & their implications

- Digitalization is promoted to enhance transparency and reduce the use of cash.
    - It helps to make it easier to track and monitor financial transactions.
- Digital transactions can be vulnerable to cyber-attacks, phishing, and fraud.
    - This needs strong cybersecurity measures to protect digital financial systems.
- Digitalization can increase the reach of financial services to remote areas.
    - This promotes financial inclusion and reduces reliance on informal financial channels.
- Digital transactions create data trails that can be used for analysis.
    - Big data analytics and AI can help to identify patterns of money laundering.
- The Digital Personal Data Protection Act, 2023 was passed to protect personal data.
    - The Data Protection Board of India will enforce the act.
- The use of technology can also aid in the detection of fake news.
    - Artificial Intelligence (AI) can help identify the source of fake news.

4) Role of Banking Sector and Other Financial Institutions

- **Banks** and other financial institutions are essential in identifying and reporting suspicious transactions.
    - They are required to authenticate client identities, keep records and provide information.
    - They need to have a system for reporting financial activity to FIU-IND.
- **Financial institutions** must adhere to the guidelines of the Prevention of Money Laundering Act (PMLA).
    - They are included in the definition of "reporting entities" under PMLA.
- The **Basel Committee** on Banking Regulations has a ‘statement of principles’ to prevent banks from hiding illicit funds.
- It aims to ensure that banks are not used for laundering money.
- **Payment system operators** like full-fledged money changers, money transfer services and Master Card are reporting entities.
- They are obligated to report suspect financial activity.
- The **Financial Action Task Force (FATF)** sets standards to combat money laundering and terrorist financing.
    - It promotes effective implementation of legal, regulatory, and operational measures.
- **International Organisation of Securities Commission (IOSCO)** advises its members to prevent money laundering in securities markets.
    - It sets global standards to promote integrity in the securities and futures markets.

5) KYC Norms and Their Significance

- **Know Your Customer (KYC)** norms are crucial to verify client identity and address money laundering.
    - They help in authenticating the identity of clients.
    - KYC helps prevent misuse of financial systems.
- **KYC compliance** is mandatory for banking companies, financial institutions, and intermediaries.
    - These institutions must maintain records of transactions.
    - They are required to provide information to the Financial Intelligence Unit-India (FIU-IND).
- **KYC norms** promote transparency, reduce fraud and strengthen the integrity of the financial system.
- This helps prevent the use of financial systems for illicit purposes.
- **Recent PMLA amendments** widened the ambit of reporting entities to incorporate more disclosures from NGOs.
    - It brought practicing chartered accountants, company secretaries, and cost and works accountants into the ambit.

- **Lowering the threshold for beneficial ownership** is also a recent change to PMLA for better transparency.
- This helps to reveal the true owners of funds and assets.

International Level Measures

1) FATF (Financial Action Task Force) and its Role

- The **Financial Action Task Force (FATF)** is an intergovernmental organization established in 1989 by the G7.
    - It aims to set standards and promote effective implementation of measures to combat money laundering and terrorist financing.
- **FATF** has formulated a series of recommendations that have become international standards.
    - These standards are used to fight against money laundering, terrorist financing, and threats to financial system integrity.
- **India is a member of the FATF** and is committed to implementing its recommendations.
    - This demonstrates India's commitment to international cooperation in combating financial crimes.
- **FATF recommendations** provide a framework for countries to develop their anti-money laundering policies and procedures.
    - These recommendations also help in the prevention of financing the proliferation of weapons of mass destruction.

2) International Cooperation and Treaties

- **International cooperation** is essential because money laundering is a large-scale activity with international scope.
    - It requires collaboration and strict, uniform laws among all countries.
- **The Multilateral Competent Authority Agreement (MCAA)** was developed for Automatic Exchange of Information as per Common Reporting Standards (CRS).
    - This enables countries to exchange financial information.
- The **Council of Europe Convention (1990)** establishes a common money laundering policy.
    - It facilitates cooperation in investigation, search, seizure, and confiscation of proceeds of crime.
- Several **United Nations Conventions** also address money laundering.
    - These include the International Convention for the Suppression of the Financing of Terrorism (1999), UN Convention against Transnational Organized Crime (2000), and UN Convention against Corruption (2003).
- **Bilateral agreements** can promote research and information sharing on cyber security which helps in combating money laundering.
- These agreements can include developed nations such as the US, Singapore, Israel, and Japan.

3) Role of Interpol and Other International Agencies

- **Interpol**.
- **The Financial Intelligence Unit (FIU)** is responsible for coordinating and strengthening international intelligence efforts.
    - It is a key agency in the global effort against money laundering and related crimes.
- **International bodies** like the United Nations Global Programme Against Money Laundering (GPML) help combat money laundering.
    - GPML provides technical assistance and complete cooperation services to governments.
- **The Vienna Convention (1988)** was the first major initiative in the fight against money laundering.
    - It requires member states to criminalize the laundering of proceeds from drug trafficking.

4) Information Sharing Mechanisms

- **Automatic Exchange of Information** through the MCAA is a critical information sharing mechanism.
    - This allows countries to receive information about accounts held by their residents in other jurisdictions.
- **Financial institutions** are required to provide information on suspicious transactions to the Financial Intelligence Unit (FIU-IND).
    - This includes banks, companies, and intermediaries.
- **Effective anti-money laundering** requires coordination between federal and state governments.
    - It also involves making beneficial ownership information more transparent.
- **International cooperation** helps ensure that competent authorities can share information regarding money laundering, terrorism financing, and predicate offenses.
    - This sharing of information makes the investigation process quick and effective.
- **A robust system** is needed to identify suspicious activities and huge transactions without legal reason.
    - This can prevent the use of financial systems for illicit activities.

Emerging Challenges & Trends

1) Technological Advancements (Crypto-currencies, Online Gambling)

- **Technological progress**, including cyber technologies, makes it difficult to detect money laundering.
    - Law enforcement struggles to keep pace with the rapid expansion of these technologies.
- **Emerging technologies** and globalisation contribute to money laundering by enabling faster and concealed transfers.
    - They help disguise the illegal source of money.
- **Crypto-currency transactions** have been brought under the ambit of the Prevention of Money Laundering Act (PMLA) recently.
    - This is to combat the misuse of virtual assets for money laundering.
- **Online gambling** is also a channel for money laundering, requiring new measures to tackle it.
    - It involves the movement of money through digital platforms, making detection harder.
- **Artificial intelligence (AI)** and **machine learning** can be used for better prediction and identification of digital security attacks and breaches..
    - AI can be used in tackling money laundering.
    - Big data analytics can also be used in tackling money laundering.

2) Globalization and its Impact

- **Globalization** facilitates money laundering by enabling faster transmission of money.
    - It helps conceal the source of the money from its illegitimate origin.
- **Cross-border money flows** and **tax avoidance** are aided by money laundering, undermining economic sovereignty.
    - It poses a serious threat to a country's economic stability.
- **The integration of the global financial system** integrates both positive and negative elements related to money laundering.
    - It allows illicit funds to be moved quickly through various international accounts.
- **Increased international trade and capital flows** make it easier for criminals to move money across borders.
    - This requires international cooperation to track illicit financial activity.
- **Money laundering** is aided by informal cross-border money flows and tax avoidance issues.
    - It impacts the financial integrity of a nation.

3) Use of Shell Companies and Tax Havens

- **Shell companies** are used to disguise the origin of illegal money through complex transactions.
    - They often have no real business operations.
- **Tax havens** facilitate money laundering by offering low or zero taxation and financial secrecy.
    - These jurisdictions are often used for illicit financial transactions.
- **Offshore financial centers** are used to move money through complex structures to evade taxes.
    - These centers specialize in non-resident financial transactions.
- **Multinational corporations** use networks of corporate entities to artificially move income to low-tax areas.
    - These methods help in taking advantage of the low-tax systems.
- **The use of shell companies** to conduct business operations in secrecy, allows for fake invoices and balance sheets.
    - It is an important method of layering in money laundering.

4) Political Factors/Corruption

- **Corruption** creates a cycle where black money is generated, encouraging further corruption.
    - This corruption can also be a driver for money laundering activities.
- **Political instability** and lack of transparency can increase vulnerabilities to money laundering.
    - It allows illicit activities such as drug trafficking and smuggling to flourish.
- **Politically exposed persons (PEPs)** are a new category defined in PMLA to monitor their financial transactions.
    - This is an effort to enhance transparency and reduce corruption.
- **Weak governance** and lack of accountability can enable money laundering activities.
    - A lack of public awareness also contributes to the issue.
- **Hawala**, an informal low-cost money transfer technique, is used to move funds without formal institutions.
    - It is often used to evade scrutiny.
- **The main sources of money laundering** include illegal activities, cyber fraud, corruption and drug trafficking.
    - These crimes often take place because of political instability.

Case Studies (Indian & Global)

1) Real-world Examples of Money Laundering Cases (e.g., specific scams or instances)

- **Money laundering** is used to conceal the illegal sources of income from activities like drug trafficking, and extortion.
    - It involves disguising the origins of funds to make them appear legitimate.
- **Illegal activities** within a country such as cyber-enabled fraud, corruption, and drug trafficking are the main sources of money laundering.
    - These activities generate illicit proceeds that are then laundered.
- **Narcotics trafficking and smuggling** are used to fund terrorist networks.
    - This shows how money laundering supports other criminal activities.
- **Hawala** is an informal money transfer system that is often used for money laundering.
    - It facilitates the movement of funds without leaving a clear audit trail.
- **Shell companies** are used to create fake invoices and balance sheets to hide the origin of funds.
    - These companies often conduct business in secrecy to disguise money laundering operations.
- **The 2019 judgement on the PMLA** highlighted that money laundering cannot be considered less severe than terrorism.
    - This shows the gravity of the crime and its impact on security.

- **The use of shell companies** to conduct business operations in secrecy, allows for fake invoices and balance sheets.
- It is an important method of layering in money laundering.
- **Cyber-enabled fraud** is a significant contributor to money laundering.
    - Cyber-attacks and digital fraud schemes are difficult to trace and combat.
- **The Enforcement Directorate (ED)** is an Indian law enforcement and economic intelligence agency tasked with combating money laundering.
    - The ED has the power to seize property if it is proven to be proceeds of crime.

2) How Different Countries Have Tackled Money Laundering

- **International cooperation** is essential to combat money laundering, given its international nature.
    - Countries need to collaborate and enact strict, uniform laws.
- **The Financial Action Task Force (FATF)** is an intergovernmental body that sets standards for combating money laundering.
    - India is a member of FATF, which makes recommendations for combating the financing of terrorism.
- **The Vienna Convention** was the first major initiative in the fight against money laundering.
    - It established measures to combat money laundering from drug trafficking.
- **The Basel Committee's Statement of Principles** urged banks to adopt a viewpoint that prevents the use of banks to hide funds.
    - This sets a standard for banking regulation.
- **The Council of Europe Convention** established a common policy to facilitate cooperation in investigating money laundering.
    - It also standardizes the definition of money laundering and ways to combat it.
- **The Multilateral Competent Authority Agreement (MCAA)** is developed for Automatic Exchange of Information, according to Common Reporting Standards (CRS).
    - This helps in international tax cooperation.
- **The United Nations Global Programme Against Money Laundering (GPML)** aims to increase the effectiveness of international anti-money laundering.
    - The GPML provides tools to help countries combat money laundering.
- **A robust system** is required to detect suspicious activities and identify transactions that have no apparent economic or legal reason.
    - This includes having proper monitoring and reporting procedures in place.
- **The Prevention of Money Laundering Act (PMLA), 2002** is a comprehensive law to combat money laundering and confiscate related property.
    - It defines the offense of money laundering and provides for stringent measures.
- **The PMLA was amended** to define politically exposed persons (PEPs), lower the threshold for beneficial ownership, bring crypto transactions under its ambit and widen the ambit of reporting entities to incorporate more disclosures for NGOs.
    - These amendments aim to enhance the law's efficacy in tackling modern forms of money laundering.
- **The apex court upheld several provisions** of the PMLA in the Vijay Madanlal Choudhary vs Union of India case.
    - This includes the sections relating to attachment, search, and seizure of properties.

Case Studies (Other Countries)

Country	Main Focus/Approach	Specific Measures/Laws	Outcomes/Effectiveness	Lessons for India	Related Concepts

United States	Focus on financial institutions and strong legal framework.	* Bank Secrecy Act (BSA) and its amendments. * Office of Foreign Assets Control (OFAC) for sanctions. * Use of "Know Your Customer" (KYC) and Customer Due Diligence (CDD) regulations.	* High conviction rates for money laundering. * Strong system of reporting suspicious activities. * Effective in tackling large-scale, sophisticated financial crimes, but still issues with real estate & anonymous transactions.	* Importance of robust laws and regulatory compliance. * Strengthening of investigative powers of regulatory bodies like Enforcement agencies and FIU-IND.	KYC Norms, Regulatory Framework, Financial Institutions
Switzerland	Shift from banking secrecy to transparency and international cooperation.	* Adoption of Automatic Exchange of Information (AEOI) with other countries. * Collaboration with international bodies like FATF. * Strengthened due diligence requirements for banks.	* Significant decrease in the volume of illicit funds in Swiss Banks. * Enhanced international reputation in terms of financial integrity and accountability, yet some loopholes still exist.	* Gradually moving towards transparency in financial transactions * Effective international cooperation mechanisms for financial information exchange.	International Cooperation, Tax Evasion, Banking Secrecy
United Kingdom	Focus on organized crime and beneficial ownership transparency.	* Criminal Finances Act, which aims at asset recovery. * Creation of the National Crime Agency (NCA) to tackle financial crime. * Register of beneficial ownership for companies & other entities.	* Increased transparency in company ownership. * Enhanced capability to freeze and seize assets derived from criminal activity. * Still facing challenges due to complexity of financial systems.	* Implementing mechanisms to identify the real owners of companies and other entities. * Proactive approach in asset recovery and confiscation.	Organised Crime, Asset Recovery, Transparency

Singapore	Balancing economic growth with strong regulatory control and AML systems.	* Use of technology and data analytics for AML compliance. * Stringent enforcement of KYC/CDD practices. * Close collaboration between government agencies and financial institutions.	* Lower incidents of ML due to strong regulatory environment. * Known for its balance between financial innovation and regulatory oversight. * Challenges in keeping up with evolving methods of money laundering.	* Use of technology and data analytics to detect and prevent money laundering. * Focus on maintaining a strong regulatory culture across various sectors of the economy.	Technological Solutions, Regulatory Compliance, Financial Hubs
Australia	Combination of law enforcement and financial intelligence.	* Australian Transaction Reports and Analysis Centre (AUSTRAC) for financial intelligence. * AML/CTF Act for combating money laundering and terrorism financing. * Focus on "gatekeeper" sectors (lawyers, accountants, real estate agents).	* Significant success in tackling money laundering through real estate, gambling etc. * Effective law enforcement collaboration in combating ML. * Challenge of adapting to new methods of ML via crypto currency and tech platforms.	* Focusing on non-financial sectors (gatekeepers) to strengthen AML systems. * Effective utilization of financial intelligence to prevent crime.	Gatekeepers, Financial Intelligence, Law Enforcement

Border Security and Management **1**
Types of Threats: 1
Infiltration, illegal migration, cross-border crime (drugs, arms smuggling), insurgency, terrorism, UAV threats 1
India-Pakistan Border (LoC): Types & Challenges 2
India-Myanmar, India-Bangladesh and the impact of porous borders, difficult terrain, and hostile relations 4
Management Strategies: Border fencing, technology use (surveillance), intelligence, counter-insurgency ops, local community engagement, border area development, international cooperation 6
Specific Issues: Refugee crisis (Bhutan), local support for militants 7
Security Forces: Role of BSF, ITBP, Army, etc. 7
Subtopics and Concepts 8
Infiltration & Illegal Migration: Push/Pull factors, demographic changes, security risks 8
Cross Border Crime: Smuggling of drugs, arms, and counterfeit currency 9
Insurgency & Terrorism: Cross-border links, financing, safe havens 9
Maritime Security **10**
Threats: Piracy, maritime terrorism, illegal fishing, smuggling, environmental damage 10
Challenges: Large coastline, economic zones, international shipping lanes, presence of non-state actors 11
Management Strategies: Coastal surveillance, naval exercises, technology upgrades, international cooperation 11
Organizations: Indian Navy, Coast Guard, IMO 12
India's five basic principles for enhancing maritime se₹curity, as proposed at the UNSC, are: 12
Subtopics and Concepts 12
Piracy: Historical trends, impact on shipping, counter-piracy measures 12
Maritime Terrorism: Targets, methodology, challenges 13
Illegal Fishing: Impact on marine ecology, economic losses 14
Coastal Security: Surveillance tech, early warning systems, community involvement 14
Blue Economy: Balancing economic development with security concerns 15

Topic: Border Security and Management

- [ ] What are the issues involved in solving the problem of refugees from Bhutan? (96/10)
- [ ] Explain the problem of infiltration in eastern parts of India. (01/2)
- [ ] How far are India's internal security challenges linked with border management particularly in view of the long porous borders with most countries of South Asia and Myanmar? (13/10)
- [ ] How does illegal transborder migration pose a threat to India's security? Discuss the strategies to curb this, bringing out the factors which give impetus to such migration. (14/12.5)
- [ ] Border management is a complex task due to difficult terrain and hostile relations with some countries. Elucidate the challenges and strategies for effective border management. (16/12.5)
- [ ] Cross-Border movement of insurgents is only one of the several security challenges facing the policing of the border in North-East India. Examine the various challenges currently emanating across the India-Myanmar border. Also, discuss the steps to counter the challenges. (2019/15)
- [ ] For effective border area management, discuss the steps required to be taken to deny local support to militants and also suggest ways to manage favorable perception among locals. (2020/10)
- [ ] Analyze internal security threats and transborder crimes along Myanmar, Bangladesh, and Pakistan borders, including the Line of Control (LoC). Also, discuss the role played by various security forces in this regard. (2020/15)
- [ ] The use of unmanned aerial vehicles (UAVs) by our adversaries across the borders to ferry arms/ammunitions, drugs, etc., is a serious threat to internal security. Comment on the measures being taken to tackle this threat. (UPSC GS 3 2023/10 marks)

Topic: Maritime Security

- [ ] In 2012, the longitudinal marking for high-risk areas for piracy was moved from 65 degrees east to 78 degrees east in the Arabian Sea by the International Maritime Organization. What impact does this have on India's maritime security concerns? (14/12.5)
- [ ] What are the maritime security challenges in India? Discuss the organizational, technical, and procedural initiatives taken to improve maritime security. (22/10)
- [ ] 'Sea is an important Component of the Cosmos'. Discuss in light of the above statement the role of the IMO (International Maritime Organization) in protecting the environment and enhancing maritime safety and security. (2023/15 marks)

Border Security and Management

Types of Threats:

Infiltration, illegal migration, cross-border crime (drugs, arms smuggling), insurgency, terrorism, UAV threats.

- **Infiltration** across borders is facilitated by difficult terrain, porous borders, and riverine areas.
    - Enclaves and a large number of water bodies also make areas conducive to infiltration.
- **Illegal migration** causes social and economic insecurity for local communities, leading to tension.
    - There are an estimated 15-18 million illegal Bangladeshi immigrants in India.
- **Cross-border crime**, including drug and arms smuggling, is facilitated by porous borders.
    - The **Golden Triangle** and **Golden Crescent** are primary regions for illicit drug production.
    - Smuggling also involves human trafficking and counterfeit money.
    - **Terrorist groups** are also involved in smuggling arms and ammunition across national borders.
- **Insurgency** in the North-East is often linked to ethnic conflicts and porous borders.
    - Insurgent groups find refuge in neighboring countries along India's borders.
    - **The porous Indo-Myanmar border** is a route for drug and human trafficking.
- **Terrorism**, both state-sponsored and international, poses a major threat to internal security.
    - Terrorism is often motivated by fundamentalist ideologies and supported by financial networks.
    - Terrorist groups also use **drones** to transport arms across borders.
    - The "Resistance Front" is an attempt to secularize terrorism in Kashmir.
- **UAV (Unmanned Aerial Vehicle) threats** include the use of drones for smuggling and attacks.
    - Drones are used for transporting small arms across the border.
    - India is looking to acquire MQ9 Reaper drones from the USA.
- **Cyber warfare** is a growing threat that can destabilize a nation's economy and security.
    - Cyber attacks can lead to the loss of competitive information and public trust.
    - **Cyber terrorism** and cyber threats require a Cyber Crisis Management Plan.
    - **CERT-In** has the objective of securing Indian cyberspace and responding to cyber incidents.
- **Money laundering** is a serious threat to a country's economic sovereignty.
    - Money laundering is often linked to drug trafficking, gunrunning, and human trafficking.
    - The Prevention of Money Laundering Act (PMLA) 2002 was amended to define politically exposed persons and widen the scope of reporting entities.
    - **Money laundering** is considered as serious as **terrorism**.
    - The **Financial Action Task Force (FATF)** is an intergovernmental body that makes recommendations related to combating financing of terrorism.
- **Fake news** and misinformation spread through social media and other online platforms can cause unrest and violence.
    - AI can be used to identify sources of fake news.
    - Users should exercise judgment to question the source and credibility of the information.
- **Border disputes** with neighboring countries create conditions for increased security threats.
    - There are border disputes with China, Pakistan, and Nepal, among others.

India-Pakistan Border (LoC): Types & Challenges

I. Introduction: The Line of Control (LoC)

The India-Pakistan border is approximately 3,323 km long, from Gujarat to Jammu & Kashmir. The border is divided into three sectors: the IB sector, LC sector, and AGPL.

- **Definition:** The LoC is a militarized boundary line established after the 1947-48 Indo-Pakistani War. It roughly delineates the area of the former princely state of Jammu and Kashmir currently controlled by India and Pakistan. Crucially, it is *not* an internationally recognized border; it's a ceasefire line.
- **Significance:** The LoC is one of the most heavily militarized zones in the world and a consistent source of tension and conflict between India and Pakistan. It is the focal point of the Kashmir dispute.
- **Key Difference:** It's essential to distinguish the LoC from the International Border (IB), which defines the boundary between India and Pakistan in Punjab, Rajasthan, and Gujarat. The IB is a recognized international boundary.

II. Border Types Along the LoC

The LoC is not a uniform entity; it presents varying geographical and strategic challenges.

1. **Mountainous Terrain:**
    - **Example:** High altitude regions in Kargil, Siachen, and areas north of the Kashmir Valley.
    - **Challenges:**
        - **Difficult Terrain:** Rugged mountains, glaciers, and extreme weather conditions make movement and logistical support challenging for troops.
        - **Vulnerability to Infiltration:** Porous borders and unguarded passes provide opportunities for infiltration, particularly in summer months when snow melts.
        - **High Altitude Warfare:** Specialised training, equipment, and medical support are essential for military operations.
        - **Siachen Glacier:** The Siachen Glacier is the world's highest battleground; extremely expensive and dangerous to maintain troops.
        - **Data:** According to a report by the Indian Defence Ministry, the cost of maintaining troops at the Siachen Glacier is almost equivalent to a fighter squadron.
    - **Case Study:** The 1999 Kargil War highlighted the difficulties of border surveillance in the mountainous terrain and the risk of infiltration by Pakistani forces.
2. **Riverine Areas:**
    - **Example:** Regions along the Chenab and Jhelum rivers.
    - **Challenges:**
        - **Dynamic Border:** Shifting river courses alter the border demarcation, leading to confusion and potential disputes.
        - **Flooding:** Monsoon season leads to heavy flooding, making patrolling and border maintenance difficult.
        - **Cross-Border Movement:** Rivers can facilitate illegal movement, smuggling, and infiltration.
3. **Forest/Vegetated Areas:**
    - **Example:** Lower reaches of the Pir Panjal range, densely forested.
    - **Challenges:**
        - **Concealment:** Dense vegetation provides cover for infiltrators and militants.
        - **Difficult Patrolling:** The thick foliage hinders visibility, making it hard to patrol and monitor the border.
        - **IED Threats:** These areas are susceptible to the planting of Improvised Explosive Devices (IEDs).

- **News:** Regular news reports detail counter-insurgency operations in forested areas along the LoC where terrorists and infiltrators are found to have camped in forested areas.

III. Key Challenges Along the LoC

1. **Ceasefire Violations:**
   - **Data:** According to reports from the Indian and Pakistani armies, thousands of ceasefire violations have occurred over the years. In 2020 alone, India reported over 5,100 ceasefire violations.
   - **Impact:**
     - **Loss of Life:** Frequent firing incidents have resulted in casualties among civilians and security forces.
     - **Displacement:** Residents living in border villages are forced to evacuate their homes.
     - **Erosion of Trust:** Ceasefire violations escalate tensions and hinder diplomatic efforts.
     - **Examples:** Constant shelling at border villages of Poonch and Rajouri result in frequent civilian casualties.
   - **Committees & Reports:** The Parliamentary Standing Committee on Defence has repeatedly expressed concern over the frequency of ceasefire violations and their adverse impact.
2. **Infiltration:**
   - **Nature:** Cross-border movement of militants/terrorists from Pakistan-administered Kashmir into India.
   - **Methods:**
     - Utilizing natural passages in mountainous terrain.
     - Using tunnels and underground passages.
     - Exploiting unguarded areas and porous sections of the border.
   - **Impact:**
     - Fuels terrorism and insurgency in Jammu and Kashmir.
     - Undermines the peace and security of the region.
   - **Case Study:** The 2016 Uri attack, which resulted in the death of 19 Indian soldiers, was attributed to infiltration from across the LoC.
3. **Smuggling & Illegal Trade:**
   - **Nature:** Cross-border movement of narcotics, arms, and other illegal goods.
   - **Impact:**
     - Finances terrorist groups and criminal organizations.
     - Undermines local economy and development.
     - Creates a security challenge along the LoC.
   - **News:** Seizures of narcotics and weapons near the LoC are regularly reported.
4. **Humanitarian Issues:**
   - **Displacement:** Frequent conflict leads to displacement of border populations.
   - **Lack of Infrastructure:** Limited access to basic amenities like healthcare, education, and livelihood opportunities.
   - **Psychological Impact:** Constant fear and uncertainty have a devastating impact on the mental health of people living near the LoC.
   - **Case Study:** Border areas often lack necessary amenities due to frequent conflict, leading to deprivation.
5. **Landmines and IEDs:**
   - **Challenge:** Landmines laid during past conflicts continue to pose a threat to civilians and military personnel.
   - **IEDs:** Improvised Explosive Devices planted by militants create a threat, particularly in forested areas.
   - **Impact:** Fatal and disabling injuries, impeding movement in border areas.

    - **Case Study:** Regular news reports detail how security personnel and civilians suffer from landmine and IED blasts.
6. **Lack of Trust & Communication:**
    - **Challenge:** Deep mistrust between the Indian and Pakistani governments and military establishments impedes cooperation.
    - **Impact:** Hinders dialogue, escalates tensions, and makes conflict resolution difficult.
7. **Geopolitical Factors:**
    - **Challenge:** The conflict along LoC is further complicated due to the presence of other actors in the region.
    - **Impact:** External actors like China supporting Pakistan to use the proxy war to put pressure on India.

IV. Efforts to Manage the LoC

1. **Border Fencing & Surveillance:**
    - India has erected a fence along much of the LoC to reduce infiltration, along with observation posts, sensor networks and drones.
    - While effective, it has limitations in the rugged terrain and during severe weather.
2. **Military Presence:**
    - Both India and Pakistan maintain a significant military presence along the LoC.
    - This high level of militarization is very expensive and maintains a fragile status quo.
    - The government has approved the construction of 422 Composite Border Outposts along the Indo-Pakistan border
3. **Confidence-Building Measures (CBMs):**
    - Efforts to establish hotlines and border meetings to address border incidents.
    - However, CBMs have often been ineffective because of trust deficit.
    - The government has approved the construction of 422 Composite Border Outposts along the Indo-Pakistan border
4. **Cross-Border Trade & Travel:**
    - **Efforts:** Limited trade routes across the LoC, though often disrupted by tensions.
    - **Limitations:** Insufficient to foster true peace, vulnerable to geopolitical circumstances.
5. **Diplomacy:**
    - **Efforts:** Regular high-level diplomatic talks.
    - **Limitations:** Geopolitical factors and deep trust deficit make diplomatic solutions difficult to achieve.

India-Myanmar, India-Bangladesh and the impact of porous borders, difficult terrain, and hostile relations.

- The **India-Myanmar border**, spanning **1,643 km**, is characterized by **difficult terrain** including high mountains, deep river channels and dense forests.
    - This **rugged terrain** makes movement and overall development of the area challenging, hindering effective border management.
    - The border is also marked by a lack of roads and communication links, affecting rapid movement of forces.
- The **Indo-Myanmar border**, though formally demarcated, is not clearly defined on the ground, causing disputes and impacting border security.
    - The boundary is superimposed on a socio-cultural landscape, dividing several tribes and leading to cross-border ethnic linkages that insurgents exploit.
- The **Free Movement Regime (FMR)**, which allowed border tribes to travel 16 km into each other's territory without visa restrictions, has been **scrapped in 2024** due to security concerns.
    - FMR was exploited by insurgents for establishing safe havens, and for smuggling weapons and drugs.

- The **India-Bangladesh border**, India's longest terrestrial border at **4,096 km**, is also marked by a high degree of **porosity**.
    - Wide gaps between border outposts (BOPs) and a dense population near the boundary facilitate free movement of criminals.
- The **India-Bangladesh border** passes through varied terrain including plains, riverine areas, hills, and jungles, which makes border management complex.
    - The border also has a **non-linear pattern**, passing through villages, fields, and rivers, further complicating management.
- Both the **India-Myanmar** and **India-Bangladesh borders** are affected by a lack of physical barriers and infrastructure, leading to weak vigilance.
    - Smugglers often cut barbed wire fences, requiring constant maintenance and vigilance.
- **Porous borders** facilitate **illegal migration**, particularly from Bangladesh to India, causing socio-economic insecurity and tension.
    - There are an estimated 15-18 million illegal Bangladeshi immigrants in India, spread across the Northeast.
    - Difficulty in identifying Bangladeshi nationals arises because of cultural and linguistic similarities with border state populations.
- **Cross-border crime** is prevalent due to porous borders, with **drug and arms trafficking** being major challenges along the **India-Myanmar border**.
- Weapons from Thailand, Cambodia, and China are smuggled through the India-Myanmar border.
- The **Golden Triangle** makes the India-Myanmar border vulnerable to heroin and amphetamine-type stimulants (ATS) trafficking.
- **Insurgency** in the North-East is a significant threat, with groups using the **India-Myanmar border** for safe havens.
    - Insurgents have ethnic ties across the border, making it easy for them to find support.
- **Hostile relations** with neighboring countries can negatively impact border management, requiring careful political and diplomatic initiatives.
- Pakistan's ISI is implicated in using porous borders with Nepal and Myanmar to spread terrorism.
- Some elements within Bangladesh authorities are suspected of colluding with ISI.
- **Dual track policies**, such as engagement with the junta in Myanmar, are driven by strategic interests like border security and countering insurgency, but have limitations.
    - Conflict spillover from Myanmar is a concern for Mizoram and Manipur.
- **Over-population** in border areas, with densities of 700-800 persons per sq. km on the Indian side and approximately 1,000 on the Bangladesh side, adds to the challenges.
    - This population density, coupled with poverty, contributes to cross border criminal activity.
- Border management is also affected by a **lack of coordination** between central and state agencies.
- **Community interaction** programs are crucial to sensitize border communities to participate in nation-building projects.
- The **Siliguri Corridor**, with its porous borders along Bangladesh and Nepal, has become a hub for illegal activities.
- The **absence of roads and communication links** hampers movement and operations of the border guarding forces.
- The **MHA (Ministry of Home Affairs) and MOD (Ministry of Defence)** have differing views regarding the control of border guarding forces, which complicates border security.
    - MHA wants all forces under its control for a comprehensive approach, while MOD argues for the Army's continued involvement with Assam Rifles.
- **Firing across the border** occurs at the slightest provocation, adding to tension and management issues.

- **Illegal cattle trade** is another significant challenge in managing the border.
- The **lack of concern for border areas** and the belief that national development is more important have led to inadequate border management practices.
- **Artificial borders**, not based on natural features, are highly porous and hard to police.

Management Strategies: Border fencing, technology use (surveillance), intelligence, counter-insurgency ops, local community engagement, border area development, international cooperation.

- **Border fencing** is a key strategy to prevent illegal migration and cross-border activities, but is not always feasible due to difficult terrain.
    - Fencing is often cut by smugglers, and requires regular maintenance and vigilance.
- **Technology** acts as a force multiplier in border security through surveillance and monitoring.
    - This includes the use of UAVs, drones, and other sensor technology to improve vigilance.
- **Comprehensive Integrated Border Management System (CIBMS)** uses non-physical barriers where fencing is not possible.
    - CIBMS is a robust, integrated system addressing security gaps using technology.
- **Intelligence gathering** is crucial for anticipating and countering threats in border regions.
    - This involves human intelligence and technical surveillance to monitor border activity.
- **Counter-insurgency operations** are necessary to tackle militant groups operating in border areas.
    - Armed forces need enhanced legal protection to carry out these operations effectively.
- **Local community engagement** is vital for border management and national integration.
    - Sensitizing communities through interaction programs can help involve them in nation-building.
- **Border area development** projects aim to improve infrastructure and generate employment.
    - These projects seek to reduce alienation and prevent local populations from engaging in illegal activities.
- **International cooperation** is essential to manage transnational threats effectively.
    - This includes bilateral agreements for information sharing and joint operations with neighboring countries.
- **The principle of "one border, one force"** improves accountability and coordination in border management.
    - This aims to streamline operations and avoid conflicts of jurisdiction.
- **Legalizing trade** in essential commodities reduces smuggling and allows authorities to control the flow of goods.
    - This can also reduce the appeal of illicit activities and cross-border crime.
- Issuing **multi-purpose identity cards** to people in border areas helps ensure that border policy is not exploited.
    - This helps to monitor and regulate the movement of people across borders.
- The **Madhukar Gupta Committee** recommendations emphasize a technology-driven approach to border protection.
    - The committee's suggestions include border assessment, border deployment and infrastructure development.

Specific Issues: Refugee crisis (Bhutan), local support for militants.

- **Refugee crises** pose significant challenges, with India lacking a specific policy for refugees and asylum seekers.
    - A need for a policy that allows basic rights for refugees on humanitarian grounds, such as right to work, has been noted.

- **Local support for militants** is a key concern, with some communities offering logistical support and safe havens.
    - This is often driven by ethnic ties, alienation, and perceived neglect by the government.
- **Alienation** from conventional political processes can drive local populations to support insurgent groups.
    - This is due to a sense of injustice and a lack of access to power structures.
- **Racial bias** against people from the North-East in mainland India can increase the chances of youth joining insurgents.
    - The perception of being neglected can contribute to feelings of resentment and alienation.
- **Cross-border ethnic linkages** with neighboring countries provide support for insurgents and allow them to operate with relative ease.
    - This means insurgents can easily find safe havens and logistical support across the borders.
- **The presence of illegal settlers** related to certain communities fuels conflicts.
    - For instance, illegal settlers from Myanmar are alleged to be behind clearing forests for poppy and cannabis cultivation.
- **Corruption** and a lack of accountability in governance can lead to distrust and increase support for insurgents.
    - This is especially a problem where there is a nexus between political and insurgent groups.
- **Prolonged use of AFSPA** can lead to human rights violations and alienate local communities.
    - It has been reported that security forces personnel are involved in incidents of Human Rights Violations.
- The influence of insurgent groups like NSCN is still present in the regions, and they arrange their resources through extortion.
- **Lack of development** and education leads to a feeling of neglect and increases the risk of youth joining insurgent groups.
- **Grievances must be addressed** in a timely and appropriate way to prevent people from supporting militants.
    - This involves understanding the root causes of discontent and implementing measures to alleviate those issues.

Security Forces: Role of BSF, ITBP, Army, etc.

- The **Border Security Force (BSF)** is the primary force for guarding India's land borders and preventing cross-border crimes.
    - BSF's main role is to protect international borders and support the Army during war.
- The **Indo-Tibetan Border Police (ITBP)** is responsible for guarding the Sino-Indian border.
    - The ITBP also works to prevent illegal immigration and trans-border smuggling.
- The **Indian Army** plays a key role in counter-insurgency operations in border areas and assists in border protection.
    - The Army needs special powers in disturbed areas to tackle both domestic and foreign terrorists.
- The **Assam Rifles (AR)** is the oldest paramilitary force and is responsible for maintaining security in the North-East.
    - AR's mission is to fight insurgency and conduct border security operations in India's north-eastern regions.
- The **Central Reserve Police Force (CRPF)** is responsible for internal security and assisting state police in maintaining law and order.
    - The CRPF also helps in counter-insurgency operations and maintaining order in disturbed areas.

- The **National Security Guard (NSG)** is a specialized force for counter-terrorism activities, intervening in terror attacks.
    - NSG is a 'zero-error' force capable of handling terror attacks and hostage situations.
- **Sashastra Seema Bal (SSB)** guards the Indo-Nepal and Indo-Bhutan borders and prevents cross border crimes.
    - SSB is also tasked to prevent illegal entry and movement of people across the borders.
- The **Indian Coast Guard** is responsible for maritime security and protecting India's maritime interests.
    - The Coast Guard also ensures safety and security of ports, fishing zones, and offshore installations.
- **Village Volunteer Forces (VVFs)** can be a great asset in border management by providing local knowledge.
    - VVFs have had success in areas they have been implemented and should be promoted further.
- The **Cabinet Committee on Security** oversees the entire internal security apparatus, including border management.
    - The committee coordinates policy and resource allocation for border security operations.
- The **Ministry of Home Affairs (MHA)** manages operational aspects of border security and internal security.
    - The MHA is responsible for the deployment and administration of the Central Armed Police Forces.
- The **Cabinet Secretariat** and the **Prime Minister's Office (PMO)** play a key role in coordinating border management efforts.
    - These bodies help in ensuring that all involved agencies work together effectively.
- There is a need to clearly earmark the responsibilities of guarding the border between the various agencies.
- This will ensure greater clarity and reduce conflicts between agencies and forces.
- **Border guarding forces** should be primarily employed for guarding borders and not for counter insurgency or law and order.
    - This will allow the forces to focus on their primary duty of securing the borders.
- There is a need for all Central Police Organizations (CPO) like ITBP and AR to have the same powers under the Customs Act and CrPC as BSF.
    - This will lead to better coordination between the border guarding forces.
- The **Assam Rifles** should not be controlled by the MHA, as this would confuse and jeopardize security in the Northeast.
    - The Assam Rifles should retain the dual control structure, being under both MHA and Ministry of Defense.
- The Indian Army has sought total control of the **Assam Rifles** and operational control over the ITBP.
    - The ITBP is currently engaged in a standoff with the Chinese PLA in eastern Ladakh.

Subtopics and Concepts

Infiltration & Illegal Migration: Push/Pull factors, demographic changes, security risks.

- **Illegal migration** is driven by factors such as economic opportunities, availability of land, and social networks.
    - Discriminatory laws and religious persecution in neighboring countries are push factors.
- **Porous borders** facilitate the movement of illegal immigrants, posing security challenges to India.
    - India's border with Bangladesh and Nepal are particularly porous.
- **Demographic changes** due to illegal immigration cause social and economic insecurity among local communities.

    - There are estimated to be 15-18 million illegal Bangladeshi immigrants in India.
- **Illegal settlers** from Myanmar are involved in clearing forests for opium cultivation.
    - These settlers are ethnically related to the Kuki-Zomi people of Manipur.
- **Lack of a definite policy** for refugees and asylum seekers creates uncertainty and deprives them of basic rights.
    - India should consider giving the right to work and identity cards to refugees on humanitarian grounds.
- **The Siliguri corridor**, with porous borders along Bangladesh & Nepal, has become a hub for illegal activities.
    - This corridor is also used for the infiltration of third country nationals.
- **Tighter border controls** are needed to curb illegal migration by making it difficult for people to cross without permission.
    - Border surveillance must be improved with better patrolling and monitoring.
- **Border fencing** is a method for preventing illegal migration and should be erected at strategic locations.
    - Roads should be built to make security patrols easier and prevent illegal crossings.
- **The open border regime** with Nepal and Myanmar has become a problem for security agencies.
    - It allows drug traffickers and smugglers to move freely across the borders.

Cross Border Crime: Smuggling of drugs, arms, and counterfeit currency.

- **Smuggling of drugs, arms, and counterfeit currency** is a major security challenge along India's borders.
    - These activities fund criminal and terrorist groups.
- **Drug trafficking** is linked to other illicit activities like gunrunning, money laundering and human trafficking.
    - The **Golden Triangle** and **Golden Crescent** are major sources of illegal narcotics.
- **The Indo-Myanmar border** is a route for drug trafficking, as it is close to the Golden Triangle.
    - This border is also used for the trafficking of women and young children.
- **Counterfeit money** is used to fund crime and terrorism, posing a threat to economic security.
    - The smuggling of fake currency facilitates black money and money laundering activities.
- **Smuggling of arms** is done across borders and creates a threat to internal security.
    - These arms are often used by insurgents and terrorists.
- **The use of drones** to transport weapons and drugs across the border has emerged as a new challenge.
    - Small arms are often transported across the border using drones.

Insurgency & Terrorism: Cross-border links, financing, safe havens.

- **Insurgent groups** in the North-East have cross-border links and are supported by elements in neighboring countries.
    - These groups use porous borders to their advantage by conducting operations in India and hiding.
- **Terrorist groups** receive support from across the border, including training, financing and safe havens.
    - Pakistan has been identified as a primary source of terrorism in the region.
- **Terrorist financing** is done through both legitimate and illegitimate sources.
    - Money laundering is a key method used to finance terrorist activities.
- **Drug money** is used by terrorist groups to fund their operations.
    - Narcotic trade is systematically aided to fund terrorist outfits.
- **Cyber warfare**, often state-sponsored, poses a major threat to national security.

- Cyber-attacks can destabilize the country and have a significant impact on internal security.
- **The ideology** of terrorist groups is spread through propaganda and radical discourse.
    - Social media is often used as a tool for spreading propaganda and recruiting new members.
- **Terrorism** is often motivated by fundamentalist ideologies.
    - These ideologies are supported by efficient but secretive financial networks.
- **The concept of invisible warfare** is used to destabilize a country through misinformation, cyber-attacks, and social engineering.
    - Invisible warfare is also called fifth generation warfare or non-kinetic warfare.
- **Terrorism** aims to create fear and use violence to achieve a political, religious, or ideological goal.
    - It has an insidious effect on the people and creates an atmosphere of fear.
- **The National Investigation Agency (NIA)** is a positive move in addressing the threat of terror financing and organized crime.
    - The NIA helps in dealing with such situations effectively.
- **The Armed Forces Special Powers Act (AFSPA)** is a tool to deal with extraordinary law and order situations perpetrated by insurgents.
- The act provides enhanced legal protection for the armed forces deployed in counter-insurgency roles.
- **Hot pursuit and Surgical Strikes** are quick and accurate actions designed to neutralize a specific target.
    - These strikes help in causing minimal collateral damage.
- **India** needs a strategy that includes strong political resolve, aggressive action, and propaganda machinery to combat terrorism.
    - The country needs to address the root causes of terrorism and ensure that no one is exploited by terrorist groups.
- **A multi-pronged approach** is needed to address terrorism with a focus on socioeconomic development.
    - The government needs to ensure that the most vulnerable are not exploited by terrorist groups.

Maritime Security

Threats: Piracy, maritime terrorism, illegal fishing, smuggling, environmental damage.

- **Maritime security** is crucial due to India's extensive coastline of over 7,000 km.
    - This underlines its importance for India's national security.
- **Piracy** is a significant threat, with incidents impacting trade and security.
    - Piracy in Somalia increased insurance prices for Indian cargo companies.
- **Maritime terrorism**, can cause massive damage and disrupt trade routes.
    - The 26/11 Mumbai terror attacks highlighted the vulnerability of the coast.
- **Smuggling and trafficking** are major concerns, with goods like gold, narcotics, and arms being transported.
    - Indian coasts have been susceptible to these activities for a long time.
- **Illegal fishing** depletes resources, affects local economies and can cause conflict.
    - Disputes and collisions involving fishing boats have led to violence.
- **Drug trafficking** through maritime routes poses a significant threat to national security.
    - The Golden Crescent and Golden Triangle are major sources of illicit drugs.
- **Environmental damage**, such as pollution and destruction of marine habitats, threatens ecosystems.

    - Conservation of the maritime environment is a key concern for India.
- **Cyberattacks** can disrupt maritime infrastructure and operations.
    - These attacks can target critical systems, causing significant damage.

Challenges: Large coastline, economic zones, international shipping lanes, presence of non-state actors.

- India has a long coastline of 7,516 km, including island territories, making it difficult to secure.
    - The coastline spans 3,331 coastal villages and 1,382 islands.
- India's Exclusive Economic Zone (EEZ) provides 30% of its resources, necessitating protection.
- The Andaman and Nicobar Islands constitute 0.2% of India's landmass but a large EEZ.
- **International shipping lanes** in the Indian Ocean are vital for trade, so their security is paramount.
    - Securing Sea Lanes of Communication (SLOCs) is important for India.
- **Choke points**, like the Strait of Hormuz and Malacca, are vulnerable and need to be secured.
    - These points are critical for global trade routes.
- **Non-state actors**, including terrorist groups, pose threats that require constant vigilance.
    - These actors often operate outside accepted international norms.
- **The presence of multiple agencies** involved in maritime security requires coordination to avoid conflicts.
    - The National Maritime Security Coordinator (NMSC) is meant to streamline governance.
- **Inadequate infrastructure** and technology in coastal areas hamper effective surveillance.
    - The Coast Guard uses Chain of Static Sensors for real-time monitoring.
- **Porous borders** and limited surveillance make it easier for illicit activities.
    - India's borders are long and winding making them difficult to secure.
- **The need to balance security concerns** with economic activities like fishing presents a challenge.
- New laws compel ships to choose routes to avoid fishing areas.

Management Strategies: Coastal surveillance, naval exercises, technology upgrades, international cooperation.

- **Coastal surveillance** is enhanced through the establishment of a network of radars and sensors.
    - The Indian Coast Guard has established 46 radars for real-time coastal monitoring.
- **Naval exercises** with other countries help in building interoperability and strengthening maritime security.
    - Joint exercises promote cooperation in addressing threats from non-state actors.
- **Technology upgrades**, such as drones and other sensors, are crucial for effective maritime surveillance.
    - Greater use of technology such as UAVs is needed as a force multiplier.
- **International cooperation** is vital for addressing transnational crimes and maritime security threats.
    - India proposed five basic principles for enhancing maritime security at UNSC.
- **The National Maritime Security Coordinator (NMSC)** was appointed to streamline maritime governance.
    - The NMSC works under the National Security Advisor (NSA).
- **A unified maritime command** has been created, headed by the Indian Navy, for better security.
    - This command ensures integrated maritime security.

- **The Comprehensive Integrated Border Management System (CIBMS)** covers areas where physical fencing isn't feasible.
    - CIBMS uses non-physical barriers to manage borders.
- **The use of Artificial Intelligence and Machine Learning** can help in better prediction of digital security breaches.
    - These technologies can identify digital security attacks and breaches.
- **A need for a security oriented approach** between police and intelligence to address causes of terrorism.
    - This approach also aims to address the root causes of terrorism and its spread.

Organizations: Indian Navy, Coast Guard, IMO.

- The **Indian Navy** plays a key role in maritime security, protecting the nation's interests.
    - The Indian Navy heads the unified maritime command.
- The **Indian Coast Guard (ICG)** is responsible for safeguarding India's maritime zones.
    - The ICG was established under the Coast Guard Act, 1978.
- The **International Maritime Organization (IMO)** sets international standards for maritime safety and security.
    - The IMO is an agency of the United Nations.
- The **National Security Council (NSC)** is an apex body that deliberates on all aspects of national security.
    - The Prime Minister heads the NSC.
- The **National Security Advisor (NSA)** serves as the secretary of the National Security Council.
    - The NSA also heads the National Security Advisory Board (NSAB).
- The **National Security Advisory Board (NSAB)** undertakes long-term analysis of security issues.
    - NSAB provides perspectives on national security issues to the NSC.
- The **Strategic Policy Group (SPG)** is the principal forum for coordination and integration of inputs.
    - The Cabinet Secretary chairs the SPG.
- The **Indian Computer Emergency Response Team (CERT-In)** is responsible for cybersecurity incident response.
    - CERT-In issues directions related to cybersecurity.
- The **Multi-Agency Centre (MAC)** shares intelligence with concerned agencies in states.
    - MAC is not responsible for gathering intelligence.

India's five basic principles for enhancing maritime se₹curity, as proposed at the UNSC, are:

1. **Removal of barriers to maritime trade**.
2. **Resolution of maritime disputes peacefully** and in accordance with international law.
3. **Jointly tackling maritime threats** from non-state actors and natural disasters.
4. **Conservation of maritime environment** & marine resources.
5. **Responsible maritime connectivity**.

Subtopics and Concepts

Piracy: Historical trends, impact on shipping, counter-piracy measures.

- **Piracy** has historically been a threat in the Indian Ocean, impacting trade routes and economies.
    - In 2012, the longitudinal marking for high-risk areas for piracy was moved from 65 degrees east to 78 degrees east in the Arabian Sea.
- **Piracy incidents** disrupt shipping, increase insurance costs, and threaten the safety of crews.

    - Insurance prices for Indian cargo companies have risen, resulting in an increase in trade along the coast.
- **Counter-piracy measures** include increased naval patrols, international cooperation, and legal frameworks.
    - India is demanding the rollback of international guidelines which designate seas close to its western coast as at high risk of piracy.
- **Private security** has been used on some vessels, posing challenges and creating security problems.
    - In Indian seas, many vessels began to embark privately contracted armed guards, posing severe security problems.
- **The Lakshadweep area** in the Arabian Sea is particularly vulnerable to piracy, requiring enhanced protection.
    - Following an increase in piracy near Somalia, which extended as far as Lakshadweep, industry bodies collaborated with the IMO.
- **The Contact Group on Piracy off the Coast of Somalia (CGPCS)** was created to address piracy in the region.
    - The revised classification brought the high-risk zone significantly closer to the Indian shore.
- **New laws** have forced some ships to choose routes that avoid intensive fishing zones.
    - This has resulted in an upsurge of violence in the adjacent seas.

Maritime Terrorism: Targets, methodology, challenges.

- **Maritime terrorism** targets ports, ships, and offshore installations, causing significant damage and disruption.
    - The 26/11 Mumbai attacks demonstrated the vulnerability of India's coast to terrorism.
- **Terrorist groups** use maritime routes for smuggling weapons, explosives, and personnel.
    - These routes are also used for drug trafficking and other illicit activities.
- **The methodology** of maritime terrorism includes attacks on oil platforms, ports, and passenger vessels.
    - These attacks can be sophisticated and coordinated, causing widespread fear and panic.
- **Challenges** in countering maritime terrorism include identifying potential threats and coordinating responses.
    - The involvement of non-state actors makes it difficult to predict and prevent attacks.
- **The use of technology**, such as social media platforms and encrypted messaging applications, is used to recruit and coordinate terrorist activities.
    - Terrorists use the internet to spread propaganda, impact psychological warfare, and recruit new members.
- **Coordination** among various security agencies and intelligence sharing are crucial to addressing the challenge of maritime terrorism.
    - The Multi-Agency Centre (MAC) shares intelligence with agencies.
- **A security-oriented approach** is needed to address the root causes of terrorism and counter the spread of extremist ideologies.
    - This approach requires coordination between police and intelligence agencies.
- **Cyberattacks** on maritime infrastructure are a growing concern for security.
    - Cyber warfare is considered by some defense analysts to be a larger threat than even Al Qaeda or terrorism.

Illegal Fishing: Impact on marine ecology, economic losses.

- **Illegal fishing** depletes fish stocks, damages marine habitats, and threatens biodiversity.
    - It leads to a decline in fish populations and disrupts the marine ecosystem.

- **Economic losses** are significant, impacting livelihoods of fishermen and the fishing industry.
    - It undermines the economic stability of coastal communities.
- **Unregulated fishing practices** often involve destructive methods, harming coral reefs and other habitats.
    - These methods include bottom trawling and the use of dynamite.
- **Lack of enforcement** allows illegal fishing to continue, causing further ecological and economic damage.
    - The vastness of the ocean makes monitoring and enforcement challenging.
- **The Exclusive Economic Zone (EEZ)** is vulnerable to illegal fishing activities, impacting national resources.
    - The Andaman and Nicobar Islands provide 30% of India's EEZ.
- **Conflicts** arise between local fishermen and large-scale illegal fishing operators, causing social tension.
    - These conflicts can lead to violent confrontations and disrupt community relations.
- **The need for sustainable practices** is important for maintaining both marine ecosystems and economic benefits.
    - Measures are needed to ensure the long-term health of marine resources.
- **International cooperation** is essential to combat illegal fishing and promote responsible fishing practices.
    - This cooperation helps to monitor and enforce regulations in international waters.

Coastal Security: Surveillance tech, early warning systems, community involvement.

- **Coastal surveillance** is crucial for detecting and preventing illegal activities and potential threats.
    - A network of 46 radars has been established for real-time coastal monitoring.
- **Early warning systems** help in providing timely alerts about natural disasters and security threats.
    - These systems use satellite data, weather forecasts, and other tech to provide alerts.
- **Community involvement** in coastal security is essential for gathering local intelligence and support.
    - The concept of Village Volunteer Forces (VVFs) has shown success in border management.
- **Technology upgrades**, like drones, sensors, and AI, enhance surveillance and response capabilities.
    - Greater use of technology, such as UAVs, is needed as a force multiplier.
- **The Coastal Security Scheme (CSS)** aims to strengthen coastal infrastructure and security measures.
    - This scheme includes the establishment of coastal police stations.
- **The National Committee for Strengthening Maritime and Coastal Security** coordinates various agencies involved.
    - This committee focuses on policy formulation and implementation.
- **The Coastal Regulation Zone (CRZ) regulations** aim to protect coastal ecosystems and control development.
    - These regulations restrict activities that may harm coastal environments.
- **Joint Operation Centers (JOCs)** help in coordinating operations between various maritime security agencies.
    - JOCs enhance interoperability and effectiveness in maritime operations.
- **A strong coastal and maritime security** was needed after the 26/11 Mumbai attacks in 2008.
    - Coordinated efforts of all concerned were put in place to strengthen coastal security.
- **The National Maritime Security Coordinator (NMSC)** is responsible for liaising with coastal states and other agencies.

    - The NMSC works to streamline maritime governance.

Blue Economy: Balancing economic development with security concerns.

- The **Blue Economy** involves the sustainable use of marine resources for economic growth and jobs.
    - This includes fishing, aquaculture, tourism, and renewable energy.
- **Economic development** through maritime activities must be balanced with security concerns.
    - Unregulated activities can increase the risk of illegal fishing, smuggling, and maritime terrorism.
- **Securing sea lanes of communication (SLOCs)** is vital for India's international trade and economic stability.
    - India's exports and imports rely heavily on shipping lanes in the Indian Ocean.
- **Choke points** like the Strait of Hormuz, Bab-el-Mandeb, and Strait of Malacca require special security measures.
    - These points are critical for international trade routes and have strategic significance.
- **Modernizing the fisheries** sector is necessary to ensure food security and economic benefits for the country.
    - The Blue Revolution scheme aims to increase fish production and ensure nutritional security.
- **The Integrated Development and Management of Fisheries** is important to ensure sustainable and inclusive growth.
    - This includes support for vulnerable groups such as women and SCs/STs.
- **The "SAGAR" initiative** (Security and Growth for All in the Region) promotes cooperation and stability in the Indian Ocean.
    - This initiative emphasizes the need for a safe, secure, and stable maritime domain.
- **Maritime security** infrastructure must be improved to support economic activities and safeguard national interests.
    - This includes strengthening the navy and coast guard capabilities.
- **The National Maritime Security Coordinator (NMSC)** under the National Security Advisor (NSA) works to streamline maritime governance.
    - The NMSC coordinates maritime security efforts and addresses challenges.
- **The Coastal Surveillance Network (CSN)** provides real-time monitoring of the coastline using 46 radars.
    - This network enhances India’s ability to detect and respond to potential threats.
- **A unified maritime command** headed by the Indian Navy helps to ensure integrated maritime security.
    - This unified command allows for better coordination and response to various security threats.

Topic/Subtopic	Key Concepts/Definitions	Challenges/Issues	Strategies/Solutions	Examples/Case Studies	Linkages	Practice Problems
Border Security						

1. Infiltration	What it means, motives	Porous borders, terrain issues, lack of technology, socio-economic conditions	Border fencing, surveillance, intelligence gathering, counter-insurgency	Example case of the Indo-Bangladesh border.	Impact on internal security, cross-border crime	Analyze the effect of fencing on infiltration in different border regions
2. Illegal Migration	Definitions, push/pull factors	Socio-economic imbalance, religious persecution, political instability, lack of opportunities	Strict migration policies, border patrols, job creation in border areas, international cooperation	Rohingya crisis case study	Demographic impact, security concerns	Examine the efficacy of current policies in dealing with migration
3. Border Management	What constitutes effective BM	Complex terrain, hostile relations, cross-border crimes, insurgency	Technology implementation (UAVs, sensors), joint border patrols, local community participation, border infrastructure	Use of UAVs for surveillance on Indo-Pak border.	Internal security, geopolitical issues	Critically assess the challenges and solutions for Indo-Myanmar border management
4. Trans-border crimes	Meaning and forms	Porous borders, corruption, lack of coordination, organized crime networks	Intelligence sharing, strict vigilance, international cooperation, asset tracking	Example cases of drug smuggling routes along the border	Impact on internal security and economy	Suggest measures to counter the smuggling of counterfeit currency
5. Role of Security Forces	BSF, ITBP, Army roles	Different terrains, jurisdiction, logistical issues	Clear mandates, training, coordination, technology use	Case study of security forces tackling insurgency in the Northeast	Internal security, national security	Compare the roles of different forces in different border areas

Maritime Security						
1. Piracy	Definition, types of piracy	Sea routes, vulnerable ships, lack of coordinated response	Naval patrols, intelligence, armed escorts, international cooperation	Case study on piracy in the Gulf of Aden.	Impact on trade, insurance	Discuss the impact of piracy on shipping costs
2. Maritime Terrorism	Definition, terrorist networks	Vulnerable targets, ease of access, lack of detection	Surveillance, intelligence, naval power, international cooperation	Mumbai 26/11 attacks and use of sea routes	National security, global security	Examine the vulnerabilities of Indian coastal infrastructure to terrorism
3. Illegal Fishing	Impact on marine ecology	Open seas, lack of enforcement, lack of accountability	Surveillance, coordinated naval action, international treaties	Example of illegal fishing in the Indian Ocean	Food security, economic security, environmental damage	Suggest policies for sustainable fishing in Indian waters
4. IMO Role	IMO conventions and its role	Compliance issues, international cooperation, resource limitations	Adherence to IMO guidelines, promoting a culture of compliance, Capacity building	Impact of IMO rules on ship safety	Maritime safety, security, environmental protection	How effective are the IMO's regulations in combating piracy?

Linkages of Organized Crime with Terrorism Questions: 1
Linkages of Organized Crime with Terrorism 1
Organized Crime: 1
1) Definition, characteristics (structure, continuity, profit-driven, use of violence, corruption) 1
2) Types: Drug trafficking, human trafficking, arms smuggling, counterfeiting, money laundering, extortion, cybercrime, illegal mining 1
3) Examples/Case studies (international and domestic) 2
Terrorism: 2
1) Definition, characteristics (political motive, violence/threat of violence, aims to instill fear) 2
2) Types: Religious, political, separatist, ethno-nationalist, narco-terrorism, state-sponsored 2
3) Examples/Case studies (international and domestic) 3
Linkages of Organized Crime with Terrorism: Linkages of Organized Crime and Terrorism: Operational Support: 4
1) How organized crime groups provide logistical support: Arms, false documentation, safe havens, communication networks, recruitment 4
2) Examples/Case studies (specific instances) 4
Linkages of Organized Crime with Terrorism: Linkages of Organized Crime and Terrorism: Shared Methodologies & Tactics: 5
1) Use of violence, intimidation, planning, communication 5
2) Why terrorist groups and organized crime organizations cooperate with each other 5
National Linkages 6
Transnational Linkages 6
Causes of Terrorism: 6
Sources & Challenges: Sources: 6
Linkages of Organized Crime with Terrorism: Terrorism in India: Sources & Challenges: Specific Examples: 8
1) Operation Black Thunder (historical case study) 8
2) ISIS threat (recent trend) 8
3) Jammu & Kashmir situation (specific region focus) 8
Challenges: 9
Counter-Terrorism Measures: Government Policies: 10
Counter-Terrorism Measures: Financial Counter-Terrorism 11
Measures to Curb Terror Funding 11
FATF Guidelines 12
No Money for Terror Conference (NMFT) Objectives and Implications 12
Security Measures 12
Intelligence Gathering 12
Border Security 13
Counter-Insurgency Operations 13
Community Engagement & Rehabilitation 13
Winning Hearts and Minds, Deradicalization Programs 13
Specific Initiatives in J&K 14
International Cooperation 14
Bilateral and Multilateral Cooperation, Treaties 14

Linkages of Organized Crime with Terrorism Questions:

- [ ] What are organized crimes? Discuss the linkages of organized crimes with terrorism. (80/30)
- [ ] What was 'Operation Black Thunder'? When was it launched? What did it achieve? (88/10)
- [ ] Discuss India's policy towards international terrorism. (20 words) (03/2)
- [ ] Write about: "Terrorism: Sources in Pakistan and Afghanistan". (06/15)

- [ ] What, in your opinion, are the causes of terrorism? Suggest suitable measures to deal with the threat of terrorism in India. (250 words) (08/30)
- [ ] Religious indoctrination via digital media has resulted in Indian youth joining the ISIS. What is ISIS and its mission? How can ISIS be dangerous for the internal security of our country? (15/12.5)
- [ ] "Terrorism is emerging as a competitive industry over the last few decades." Analyze the above statement. (16/12.5)
- [ ] The scourge of terrorism is a grave challenge to national security. What solutions do you suggest to curb this growing menace? What are the major sources of terrorist funding? (250 Words) (GS 1, 17/15)
- [ ] Analyze the complexity and intensity of terrorism, its causes, linkages and obnoxious nexus. Also suggest measures required to be taken to eradicate the menace of terrorism. (2021/15)
- [ ] Discuss the types of organized crimes. Describe the linkages between terrorists and organized crime that exist at the national and transnational levels. (22/10)
- [ ] Winning of 'Hearts and Minds' in terrorism-affected areas is an essential step in restoring the trust of the population. Discuss the measures adopted by Government in this respect as part of the conflict resolution in Jammu and Kashmir. (150 words) (UPSC GS 3 2023/10 marks)
- [ ] Give out the major sources of terror funding in India and the efforts being made to curtail these sources. In the light of this, also discuss the aim and objective of the No Money for Terror (NMFT) Conference recently held at New Delhi in November 2022. (250 words) (UPSC GS 3 2023/15 marks)

Linkages of Organized Crime with Terrorism

Organized Crime:

1) Definition, characteristics (structure, continuity, profit-driven, use of violence, corruption)

- Organized crime involves **structured groups** engaging in **continuous criminal activities** for **profit**.
    - It utilizes violence, intimidation, and corruption to achieve objectives.
- **Terrorist groups** are increasingly involved in organized crime for **funding** and resources.
    - These groups utilize **illicit activities**, such as drug trafficking and smuggling, to raise funds.

2) Types: Drug trafficking, human trafficking, arms smuggling, counterfeiting, money laundering, extortion, cybercrime, illegal mining

- **Drug trafficking** is a significant link between crime and terror, with the **Golden Triangle** being a major source.
    - Opium cultivation and drug trade provide funds for terror groups and criminal networks.
- **Human trafficking** is another source of revenue, often intertwined with drug and arms smuggling.
    - Smuggling narcotics by hiding them in human body parts is a method used in human trafficking.
- **Arms smuggling** supports both organized crime and terrorist activities, posing significant security threats.
    - Easy access to weapons through illegal channels fuels conflict and violence.
- **Counterfeiting** of currency and goods erodes economic stability and funds illegal operations.
    - It provides financial resources for both crime and terrorism.
- **Money laundering** disguises the origin of illegal funds from criminal activities.
    - It helps to integrate illegal money into the formal economy.
- **Extortion** provides another funding source, often using violence to coerce individuals.
    - It is a common tactic employed by both organized crime and terrorist outfits.
- **Cybercrime** has emerged as a tool for financial fraud and supporting other criminal activities.
    - It can be used to steal financial information, disrupt critical systems, and fund illegal operations.
- **Illegal mining** is a source of revenue for criminal elements, which may also fund terror.
    - It contributes to environmental degradation and lawlessness.

3) Examples/Case studies (international and domestic)

- **Taliban** uses **drug trade proceeds** for various purposes, including arms and human trafficking.
    - The group uses the funds to destabilize the region.
- **Islamic State** and **Al-Qaeda linked groups** in and around Jammu and Kashmir engage in organized crime.
    - Regional insurgencies in the Northeast and Left Wing Extremist groups also fund from these.
- **Terrorist organizations** have made great use of social media to recruit members.
    - They use online platforms to conduct propaganda and raise funds.
- **Drug cartels** and other criminal organizations are becoming increasingly intertwined.
    - These groups use established infrastructure for logistics, transportation, and storage.
- **Hawala networks** are used for money laundering.
    - These networks provide channels for illegal financial activities.
- **Mumbai Terror Attacks** in 2008 used VoIP phone services, for example, were used during the attacks.
    - These encrypted communications were difficult for the intelligence agencies to decipher.
- **India's** proximity to opium-growing regions enhances its internal security concerns.
    - There is a direct connection between drug trafficking and other illicit activities.
- The **use of drones** has been seen to transport small arms across the border.
    - This also highlights the technological aspect of organized crime.
- **India** is also among the countries with the **highest illicit cultivation and production of cannabis**.
    - It is also a major drug seizure country in South Asia.

Terrorism:

1) Definition, characteristics (political motive, violence/threat of violence, aims to instill fear)

- Terrorism is defined as the use of **violence** to **terrorize people** for a **political, religious, or ideological** goal.
    - It aims to **instill fear** and has had an **effect on people globally**.
- Terrorism is characterized by **political motives, violence or threat of violence,** and aims to instill **fear**.
    - It seeks to achieve a political, religious or ideological objective through use of force.

2) Types: Religious, political, separatist, ethno-nationalist, narco-terrorism, state-sponsored

- **Religious terrorism** is motivated by religious ideologies and seeks to advance a specific religious cause.
    - It often involves fundamentalist interpretations and can lead to violent acts.
- **Political terrorism** is driven by political objectives, seeking to change or overthrow a government.
    - It can include acts of sabotage, assassination, or bombings.
- **Separatist terrorism** aims to achieve political independence for a specific region or community.
    - It involves groups seeking to create a separate nation or territory.
- **Ethno-nationalist terrorism** is rooted in ethnic or national identity conflicts, often involving violence against rival groups.
    - It can lead to civil unrest and communal violence.

- **Narco-terrorism** involves terrorist groups engaging in drug trafficking to fund their activities.
    - This is a key linkage between organized crime and terrorism.
- **State-sponsored terrorism** is when a government supports terrorist groups in other countries.
    - It is often used to destabilize rival countries or undermine their interests.

3) Examples/Case studies (international and domestic)

- **Pakistan** is identified as an **exporter of terrorism to India**.
    - Groups like **Lashkar-e-Taiba** and **Jaish-e-Mohammad** are linked to attacks.
- **Terrorist groups** in **Jammu and Kashmir** have roots in the late 1940s, when Pakistan attacked India.
    - The focus of terrorism has shifted from North Kashmir to South Kashmir.
- **The Taliban** in **Afghanistan** is a major concern as it could become a breeding ground for terrorists.
    - The group is involved in drug trade, arms and human trafficking to fund their activities.
- **The Islamic State (ISIS)** is a **Salafist-Jihadi group** seeking to restore early Islamic glory, using propaganda to recruit members.
    - ISIS has shown a competitive enterprise, having control over land, labor and support.
- **Al-Qaeda** is also a terrorist organization, and is now considered to be one of the primary sources of terror.
    - It has been involved in activities across various countries and continents.
- **Lone wolf attacks** have seen a rise globally from the 1970's to 2014, indicating a decentralization of terrorism.
    - These attacks are difficult to predict and prevent because they are often carried out by individuals.
- **The 2008 Mumbai attacks** demonstrated use of **VoIP** (Voice over Internet Protocol) communications, which are difficult to trace.
    - This highlights how technology is utilized by terrorist organizations for planning.
- **The Pathankot and Uri attacks** are examples of terrorist attacks in India, raising questions about counter-terrorism operation procedures.
    - Standard operating procedures need to be established to prevent any lapses.
- **The Terror group's name 'The Resistance Front'** is an attempt to secularise terrorism in Kashmir,.
    - This shows terrorism as a political cause rather than a religious war.
- **The Mumbai train blast, the Indian Parliament attack** are all examples of past acts of terror in India.
    - These attacks highlight the continuous threat to India.
- **The Global Terrorism Index (GTI) 2023** identifies **South Asia** as the worst affected region.
    - **Afghanistan** was the worst affected country with the **Islamic State** and its affiliates, the deadliest terrorist group.
- **Terrorism** has spread to all parts of the world with increasing sophistication in methods.
    - This poses a significant threat to stability and security.

Linkages of Organized Crime with Terrorism: Linkages of Organized Crime and Terrorism: Operational Support:

1) How organized crime groups provide logistical support: Arms, false documentation, safe havens, communication networks, recruitment.

- Organized crime groups provide **arms** to terrorist groups, **facilitating violence** and attacks by these organizations.
    - They engage in **gunrunning** and **smuggling** to provide necessary weaponry to terrorists.

- They also supply **false documentation** to terrorists, enabling them to **move across borders** and **operate covertly**.
    - This helps in maintaining **anonymity** and in **avoiding detection** from law enforcement agencies.
- Organized crime provides **safe havens** for terrorists, allowing them to **plan and coordinate attacks** without being detected.
    - These are used as **secret bases** for terrorists for regrouping and training.
- They offer **communication networks**, which provide secure means for terrorist groups to **coordinate activities** and pass messages.
    - These networks use **social media platforms** and **encrypted messaging applications**.
- Organized crime groups assist with **recruitment** for terrorist groups, bringing new members into their ranks.
    - They exploit the **vulnerability** of people for **radicalization** and **indoctrination**.

2) Examples/Case studies (specific instances).

- **Drug trafficking** is used by organized crime groups to **fund terrorist activities**.
    - The **Taliban** uses the proceeds from the **drug trade** for **smuggling** and **spreading terrorism**.
- **Illicit drug trafficking** is linked with **gunrunning, money laundering,** and **human trafficking**.
    - These activities necessitate **logistical assistance** from organized crime networks.
- **Hawala transactions** and **other informal systems** are utilized by organized crime and terrorist groups to transfer funds across borders.
    - These methods make it **difficult to track** financial flows associated with terrorist activities.
- **Fake currency rackets** are also used to generate funds for terror operations, thereby destabilizing the economy.
    - This is often used to create a **parallel economy** which **aids illicit activities**.
- **Terrorist groups** use **social media** and the **internet** to spread their ideology and **recruit** new members.
    - They use the internet for **propaganda**, **radicalization**, and **fundraising**.
- **Cyber warfare**, including attacks on computer systems, are becoming more frequent and are used for **espionage** and **disruption**.
    - Terrorists use **cyber space** to **intimidate or coerce** government and people.
- **The Golden Triangle** is a region that produces opium that finds its way into India because of weak enforcement.
    - The high incidence of **drug addiction** in the North-East is evidence of this.
- **Smuggling of narcotics** involves hiding them in human bodies, which shows the **complex links** between organized crime and terror groups.
    - These operations use established logistical infrastructure such as transport and storage.
- **Terror groups** can also exploit **cross-border trade** to bring in arms across borders.
    - **Third country nationals** may infiltrate by using routes used by organised crime networks.
- **Organized criminal networks** can help terror groups to secure **clandestine access to chemical, biological, and nuclear materials**.
    - This could lead to a large scale threat to international stability.
- **Non-state actors** may use **internet and social media** for **subversive activities** that may impact internal security.
    - This requires guidelines to be put in place for proper monitoring.

Linkages of Organized Crime with Terrorism: Linkages of Organized Crime and Terrorism: Shared Methodologies & Tactics:

1) Use of violence, intimidation, planning, communication.

- Both **terrorist groups** and **organized crime** use **violence** and **intimidation** to achieve their objectives.
    - This involves **physical harm** and **threats** to **instill fear** and **compliance**.
- Both use **systematic planning** to carry out their operations effectively.
    - They conduct **detailed preparations** to ensure the success of their activities.
- They employ sophisticated **communication methods** to coordinate actions and maintain secrecy.
    - This includes **encrypted channels** and **code words** to avoid detection by authorities.
- Both use methods such as **money laundering** to conceal the source of their funds and hide illicit activities.
    - This is often done through complex financial transactions and front companies.

2) Why terrorist groups and organized crime organizations cooperate with each other.

- **Terrorist groups** and **organized crime** cooperate due to their **mutual need for resources** and **support**.
    - They form a **symbiotic relationship** where both gain from this collaboration.
- **Organized crime** provides **funding** to terrorist groups through activities such as drug trafficking, and extortion.
    - This helps in **financing** operations and **procuring** necessary materials.
- **Terrorists** benefit from **organized crime's logistical networks** for arms, safe havens, and other operational support.
    - This allows for **easier movement** and **covert operations** for terrorists.
- **Organized crime** also offers skills in **recruitment** which can provide terrorists with new members.
    - This is done by targeting vulnerable people who can be **radicalized** and **indoctrinated** easily.
- **Criminal networks** provide **access to technology** and **communication systems**, which aids terrorist groups in planning.
    - This helps them in **coordinating attacks** and evading authorities.
- Both **criminal** and **terrorist groups** use **social media** and the **internet** to **spread propaganda, radicalize,** and **recruit** new members.
    - This makes them a major threat to internal security and global stability.
- **State-sponsored terrorism** uses organized crime networks to destabilize rival countries by aiding them with funds and arms.
    - This is a way for states to wage an **invisible war** without direct involvement.
- The **shared use of violence and intimidation** are a major binding factor that allows both groups to operate together successfully.
    - They can leverage each other's strengths to spread **fear** and **achieve their goals**
- **Terror groups** use the tactics of **organized crime** such as **kidnapping for ransom** to generate revenue and spread fear.
    - This can be a major source of funding and can destabilize regions.
- **Both groups** are involved in **human trafficking** which generates money as well as helps transport people to various regions.
    - This can lead to a violation of human rights and have severe social consequences.

National Linkages

- **Definition:** Connections and cooperation within a single country, often between different groups or entities within its borders.
- **Focus:** Domestic activities and impact; primarily confined within national boundaries.
- **Examples:**
    - **Local Crime Syndicates & Domestic Terror Groups:** A local mafia group providing funding, weapons, or safe houses to a domestic terrorist organization. For example,

an Indian criminal gang smuggling explosives to a militant group operating within India.
    - **Political Parties & Regional Businesses:** A political party in a state favoring businesses within that region through policy changes or preferential treatment for political gain. For example, a state government granting tax benefits to companies owned by political party members.
    - **Farmers' Associations & State Governments:** A farmers' organization lobbying for specific agricultural policies from the state government. For example, a farmers association negotiating subsidies with the state agricultural department.

Transnational Linkages

- **Definition:** Connections and cooperation that extend beyond national borders, involving actors from multiple countries.
- **Focus:** International activities and impact; transcending national boundaries.
- **Examples:**
    - **Global Drug Cartels:** A South American cartel smuggling cocaine to Europe via Africa with a multinational network of distributors and collaborators. For example, a Mexican cartel using a shipping company in Italy to traffic drugs.
    - **International Terrorist Networks:** An international terrorist group recruiting members and conducting attacks in multiple countries across the world, like Al-Qaeda or ISIS.
    - **International Human Trafficking Rings:** An organized criminal network kidnapping and trafficking children from Bangladesh to Europe for the purpose of sexual exploitation.
    - **Multinational Corporations & Global Supply Chains:** A US-based tech company outsourcing manufacturing to factories in China, creating a global supply chain. For example, Apple contracting factories in China for phone component manufacturing.

Causes of Terrorism:

Read from Notes on Terrorist Section

Sources & Challenges: Sources:

1) Pakistan, Afghanistan, other countries.

- **Terrorism** in India is significantly influenced by **external state actors** like **Pakistan**, which is an **exporter of terrorism**.
    - Groups such as **Lashkar-e-Taiba** and **Jaish-e-Mohammad** operate from Pakistan.
- **Afghanistan** can be a **breeding ground for terrorists** as seen with the **Taliban's** use of **drug trade** to fund terror activities.
    - The **Golden Crescent**, including Afghanistan, is a major source of **opium production**.
- **Cross-border movement** of insurgents is facilitated by **porous borders**, creating security challenges for India.
    - This is especially significant along the **Indo-Myanmar border**.
- **State-sponsored terrorism** uses organized crime networks to destabilize rival countries with funds and arms.
    - This is a way for states to wage an **invisible war** without direct involvement.
- **Terrorist groups** in **Pakistan** and **Afghanistan** have a history of evolving from being locally focused to becoming globally active.
- Groups like **Al-Qaeda**, have been founded in **Peshawar**, Pakistan.
- The **Southern region of Afghanistan** is a key area for **terrorist activities**, impacting neighboring regions and countries.
    - Key areas include Kabul, Khost, Jalalabad, Gardez, and the Waziristan Mountain region.

- **India's proximity** to major **opium-producing** regions, including the **Golden Triangle** (Myanmar), increases internal security concerns.
    - This leads to increased **drug trafficking**, **gunrunning**, **money laundering,** and **human trafficking**.
- **Countries surrounding India** exploit the volatile situation and use **insurgent groups** to create instability, through funding and training.
    - They provide **military assistance** and **logistical support** to such groups.
- **Bilateral agreements** with countries such as the US, Singapore, Israel, and Japan help in **research and information sharing**.
    - This is essential for countering cyber threats and terrorism.

2) Internal factors – social, religious and political conflicts.

- **Social issues** such as **poverty**, **illiteracy**, **high youth unemployment**, and **poor governance** are drivers of terrorism.
    - These issues cause **disaffection** and can be exploited by terrorist groups.
- **Religious fanaticism**, and **communal and political polarization**, are also major drivers of terrorism.
    - These can create a **fractured society** and can be exploited by insurgents.
- **Marginalized communities** and **human rights abuses** may lead to individuals joining insurgent groups.
    - This can include the use of **racial bias** against certain communities that leads to a **perception of neglect**.
- **Prolonged delays** in the **criminal justice system** and **corruption** can also contribute to social unrest and terrorism.
    - This creates a sense of injustice and a lack of faith in governance.
- **Left-wing extremism** is a significant internal challenge, influenced by **ideological suspicions** and lack of development.
    - The **exploitation of indigenous people** and **tribal land rights** contribute to this.
- **Ethnic and demographic issues** such as illegal immigration and cultural linkages with other countries fuel internal conflicts.
    - This makes it easy for **insurgents** to penetrate the region.
- The **Northeast region of India** suffers from **ethnic conflicts** and **sub-regional conflicts**.
    - These conflicts are often fought in an **unconventional mode**.
- **Sectarian strife** between **Shia and Sunni** communities can fuel conflict and create a **permissive environment** for terrorism.
    - This is seen in regions such as the Middle East.
- **The influence of insurgent groups** such as the NSCN, and other groups is still prevalent in the northeast region.
    - These groups **arrange for finance** through extortion and violence.
- **Radicalization of youth**, through the use of the internet and social media, poses a significant threat.
    - This leads to **recruitment** and **indoctrination** of individuals into terrorist groups.
- The **diverse nature of India**, being a multi-religious and multi-ethnic society, can create internal security challenges.
    - This can be seen in ethnic clashes, such as the **Kuki vs Meiteis** conflict.
- The **lack of a definite policy** for **refugees** and **asylum seekers** creates uncertainty and can lead to social unrest.
    - This may lead to an **increase in the number of insurgents**.

Linkages of Organized Crime with Terrorism: Terrorism in India: Sources & Challenges: Specific Examples:

1) Operation Black Thunder (historical case study).

- **Operation Black Thunder** was a military operation conducted to **flush out terrorists** from the **Golden Temple** in Amritsar.
    - It was carried out in **1988** by **Indian security forces**.

- The operation highlighted the need for **clear strategies** in dealing with **terrorist groups** within sensitive religious sites.
    - It showed the **challenges** in maintaining **public order** while using **military force**.
- The incident underscores the significance of having **well-defined protocols** for security operations in such areas.
    - It showed the importance of **minimal force** while maintaining **public order**.

2) ISIS threat (recent trend).

- **ISIS (Islamic State of Iraq and Syria)** is a **Salafist-Jihadi group** that aims to **restore early Islamic glory**.
    - They are a significant threat due to their **global reach** and **ideology**.
- **Radicalization of youth** through the internet and social media is a key concern related to the ISIS threat.
    - This has led to the **indoctrination** and **recruitment** of individuals into the group.
- **ISIS uses online platforms** for **propaganda**, **communication**, and **recruitment**, making them a **major threat**.
    - They use the internet to **spread their ideology** and **plan attacks**.
- The **Salafist movement** has emerged from within the **global Jihadi movement**.
    - They aim to establish a **state** regulated by **Islamic principles**.
- **Religious indoctrination** via digital media has resulted in **Indian youth** joining ISIS, a **threat** to **internal security**.
    - This highlights the need to **counter the use of online platforms** by terrorist groups.
- **Terrorist groups** use the internet to **brainwash** youth by providing them with attractive **remuneration**, which compels them to join.
    - This makes them susceptible to terrorist ideology.

3) Jammu & Kashmir situation (specific region focus).

- The **roots of insurgency** in **Jammu and Kashmir (J&K)** can be traced back to the **late 1940s** when Pakistan attacked India.
    - The aim of the attack was to **capture the region**.
- **Militancy in J&K** has evolved, with **North Kashmir** seeing reduced violence and the **epicenter** shifting to **South Kashmir**.
    - There has been an **uptick** in **terrorist actions** in **Srinagar**, but violence has been reduced drastically overall.
- **Infiltration** across the border has significantly decreased.
    - In **2022**, until April, there were only **two infiltration attempts**.
- **Terror groups** are now trying to **communalize the valley**, with **The Resistance Front** attempting to portray the conflict as a political cause instead of a religious war.
    - This indicates an attempt to **secularize terrorism** in the region.
- **Part-time terrorists** are more difficult to track than full-time ones, making them a security challenge in the region.
    - They can also be under the radar, making it difficult for authorities to detect them.
- **Terrorist groups** are using **small arms** often transported across the border using drones.
    - This also makes it difficult for security forces to identify and intercept them.
- The government is promoting **developmental initiatives**, such as the **Special Industry Initiative (SII J&K) 'Udaan'** and the **Prime Minister Development Package**, in the region.
    - These initiatives aim to **create job opportunities** and integrate youth into society.
- **Long-term reforms**, such as **consensus building** and the **early return of statehood** to J&K, are also being considered.
    - This aims at creating a **sustainable environment of peace** in the region.
- **Islamic State** and **Al-Qaeda-linked groups** are active in and around Jammu and Kashmir, posing security threats.
    - This requires increased surveillance and counter-terrorism efforts.

Challenges:

1) Cross-border terrorism

- **Cross-border terrorism** is a major security challenge, with **terrorist groups** operating from neighboring countries.
    - This involves the **infiltration of terrorists** and the **smuggling of arms** across borders.
- **Pakistan** is identified as a key exporter of terrorism into India, supporting groups like **Lashkar-e-Taiba**.
    - These groups often engage in **sporadic attacks** aimed at causing **fear and panic**.
- **Terrorist organizations** use **drones** to transport **small arms** across borders, posing a new security threat.
    - This has made it difficult for security forces to intercept the transport of weapons.
- **India's borders** are porous, allowing for **illegal immigration**, **arms smuggling**, and **drug trafficking**.
    - The **Indo-Myanmar border**, in particular, is a route for **drug trafficking**.
- **Ethnic groups** support **cross-border terrorism**, creating a complex security environment in border regions.
    - These groups can provide **logistical support** and **shelter** to terrorists.
- **The Indo-Pak border** and **Indo-Bangladesh border** are particularly vulnerable to **infiltration** and **smuggling activities**.
    - **Composite Border Outposts** are being constructed to address these issues.
- **Border management** is a complex task due to **diverse terrain**, **ambiguous borders**, and **porous nature**.
    - This requires a coordinated effort from various agencies to secure the borders.

2) Radicalization

- **Radicalization** is the process of transforming moderate citizens into **violent extremists**.
    - It often involves the adoption of **anti-state** and **violent ideologies**.
- **Terrorist organizations** use the internet and **social media** to spread their ideology and **recruit new members**.
    - They use online platforms for **propaganda** and to **indoctrinate** and **brainwash** individuals.
- **Religious indoctrination**, particularly via digital media, has led to some **Indian youth** joining terrorist groups like **ISIS**.
    - This highlights the need to counter the use of online platforms for such activities.
- **Communalism** and **political manipulation** are factors contributing to **radicalization**.
    - **Sectarian strife** and **historical injustices** also play a role.
- **Youth** are particularly vulnerable to radicalization, due to factors like **unemployment** and **poverty**.
    - They are also easily manipulated and recruited.

3) Financing of terrorism

- **Terrorist financing** involves raising funds from both **legitimate and illegitimate sources**.
    - This includes the use of **criminal activities**, such as drug trafficking and extortion.
- **Drug and illicit trafficking** is a major source of funding for terrorist groups and has international links.
    - The **Golden Triangle** is a major source of opium, which is used to generate funds.
- **Money laundering** is used to **conceal the source of funds** and make it appear legitimate.
    - This is done through complex **financial transactions** and **transfers**.
- **Counterfeiting** is also a source of funding that also destabilizes the Indian economy.
- **Black money** generated by criminal activities is used to fund terrorist networks.
- **Hawala** is a system used for **money transfers** that makes it difficult for authorities to track the flow of funds.
    - **Extortion** and **donations** are other common methods used to fund terrorist activities.
- **FATF** is an inter-governmental body that makes recommendations relating to the **combating of financing of terrorism**.

    - India is a member of this organization.
- **The Prevention of Money Laundering Act (PMLA), 2002**, aims to tackle money laundering.
    - Recent amendments to PMLA include bringing **crypto transactions** under its ambit.
- **Financial Intelligence Unit-India (FIU-IND)** is the national agency responsible for receiving, processing, and analyzing information relating to suspicious financial transactions.
    - It is also responsible for **coordinating efforts** against money laundering.

Counter-Terrorism Measures: Government Policies:

1) India's counter-terrorism policy (domestic and international)

- India's counter-terrorism policy aims to address **domestic and international threats** through various measures.
    - This includes **intelligence gathering**, **surveillance**, and **proactive actions**.
- **Counter-terrorism operations** are undertaken after a **terrorist attack** takes place, often involving the **NSG**.
    - There have been questions about the **procedure of operations**, suggesting a need for **standard operating procedures**.
- **International cooperation** is crucial in combating terrorism, with India using forums like **UNCTC**.
    - **Bilateral agreements** with countries like the US, Singapore, and Israel also promote **information sharing** on **cybersecurity**.
- India is enhancing **counter-terrorism efforts** by **re-energizing intelligence** and strengthening infrastructure.
- This includes **tech interventions** and a focus on **socio-economic** development.
- **A multi-pronged approach** is required, combining **political**, **religious**, and **economic measures**.
    - **Counter-narratives** are essential to combat **jihadist radicalization**.
- **"Hot pursuit"** and **"surgical strikes"** are used against terrorist attacks, aiming to neutralize targets while minimizing collateral damage.
    - These actions are intended to send a **clear signal** that India will not tolerate terrorism.
- India advocates for **isolating terrorism** by ensuring it is not supported by any state or entity.
- This approach seeks to cut off all forms of support and safe havens for terrorist groups.
- A **National Cyber Security Strategy** was conceptualized in 2020, and the **Cyber Crisis Management Plan** has been developed.
    - The **National Cyber Security Policy, 2013**, also aims to create a secure **cyber ecosystem**.
- India needs a **comprehensive counter-drone capability** that includes technology and inter-forces coordination.
    - This involves creating **dedicated drone battalions** for border security and setting up **Drone Air Space Management cells**.

2) Specific legal frameworks (UAPA, NIA, etc.)

- The **National Investigation Agency (NIA)** is the key organization for investigating terrorism cases.
- It needs to be **further strengthened** to improve **prosecution and conviction rates**.
- The **Unlawful Activities (Prevention) Act (UAPA)** is used to deal with terrorist activities.
    - The **UAPA** allows the **designation of individuals as terrorists**, though there are concerns about misuse.
- **The Prevention of Money Laundering Act (PMLA), 2002**, is a comprehensive law to combat **money laundering**.
    - Recent amendments have expanded the scope of the act to include **crypto transactions**.

- The **PMLA** allows for the **temporary attachment** and **forfeiture of property** of those involved in money laundering.
    - The Act has been amended to include **politically exposed persons (PEPs)** and lower the threshold for **beneficial ownership**.
- **The Financial Intelligence Unit-India (FIU-IND)** is an autonomous body that reports on **suspicious financial transactions**.
    - It is tasked with **enforcing economic laws** and **combating illegal acts**.
- The **National Security Council (NSC)** is the apex body for deliberating on all aspects of national security.
    - It includes the Prime Minister, Ministers of Home Affairs, Defence, External Affairs, and Finance.
- **The National Cyber Coordination Centre (NCCC)** seeks to generate awareness of potential cyber security threats.
    - It also enables information sharing for **proactive** and **protective actions**.
- **CERT-In** is responsible for responding to **computer security incidents** and promoting effective **cybersecurity practices**.
    - It is the **national nodal agency** for responding to **cybersecurity threats**.
- The **Information Security Education and Awareness (ISEA)** project provides training for **information security**.
    - It aims to raise awareness among personnel about **cyber security**.
- The **Criminal Law Amendment Ordinance (XXXVIII of 1944)** covers some crimes such as corruption and cheating.
- The **Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act, 1976** allows for the forfeiture of illegally acquired property.

Counter-Terrorism Measures: Financial Counter-Terrorism

Measures to Curb Terror Funding

- Terrorism is financed through both legitimate and illegitimate sources, including companies and trusts.
    - Illicit activities, such as drug trafficking, are used to fund terrorist organizations.
- Money laundering is used to conceal the illegal sources of funds used for terrorism.
    - **Hawala**, a system of informal money transfer, is often used for terror financing.
- Terrorist groups raise funds through extortion, kidnapping, and bank robberies.
    - They also use social media platforms, blogs, and digital currencies for fundraising.
- Counter-terror financing measures include identifying and disrupting financial flows to terrorists.
    - This involves tracking suspect transactions and freezing assets linked to terrorism.
- International cooperation is essential to trace and disrupt terrorist financial networks.
    - **Financial intelligence** is crucial to understanding the financial flows of terrorist organizations.
- The **Prevention of Money Laundering Act (PMLA)**, 2002, helps to combat money laundering and terrorist financing.
    - It allows for the confiscation of property obtained through money laundering.
- A multi-pronged approach is needed to counter terror financing, including law enforcement and intelligence.
    - The **Financial Intelligence Unit-India (FIU-IND)** is an autonomous body that coordinates efforts against money laundering.

FATF Guidelines

- The **Financial Action Task Force (FATF)** sets international standards for combating money laundering and terrorist financing.
    - It formulates a series of recommendations that have become international standards in this fight.
- FATF recommendations include measures to identify, assess, and understand money laundering risks.

    - Countries must implement effective **AML/CFT** (Anti-Money Laundering/Combating the Financing of Terrorism) frameworks.
- These measures include customer due diligence, reporting suspicious transactions, and international cooperation.
    - They emphasize the need for information sharing and collaboration between nations.
- Countries should implement measures to prevent the use of the financial system for terror funding.
    - This includes scrutiny of financial institutions and Non-Profit Organizations.
- **FATF** encourages countries to adopt a risk-based approach to combat money laundering.
    - This approach focuses on the highest risk areas for terrorist financing.
- India is a member of **FATF**, and must implement its recommendations.

No Money for Terror Conference (NMFT) Objectives and Implications

- The **No Money for Terror (NMFT)** conference aims to strengthen global cooperation in combating terror financing.
    - It brings together countries to discuss and develop strategies to disrupt financial flows to terrorist groups.
- Objectives include enhancing intelligence sharing and cross-border cooperation.
    - The conference promotes the adoption of best practices in counter-terror financing.
- Implications include the tightening of financial regulations and increased scrutiny of financial transactions.
    - There is also a focus on capacity building in countries to detect and prevent money laundering.
- The conference also focuses on leveraging technology to counter terrorist financing.
    - This includes the use of artificial intelligence and machine learning for better prediction of digital attacks.
- **NMFT** emphasizes the need for a comprehensive approach to counter-terrorism that includes economic and social measures.
    - It is important to have a strategy that ensures a peace based and cohesive environment which is less susceptible to terrorist ideology.
- The conference highlights the importance of preventing the misuse of non-profit organizations for terror financing.
    - This includes greater transparency and accountability of these organizations.
- The conference underscores that countering terror financing is a collective responsibility that requires global cooperation.
    - It promotes international collaboration in investigations and allows for extradition between member states.

Security Measures

Intelligence Gathering

- Effective intelligence is crucial for preempting terrorist attacks and disrupting their networks.
    - This includes gathering human and technical intelligence to track recruitment.
- Intelligence agencies need to coordinate to share information effectively and improve analysis.
    - A strong counter-intelligence presence is vital, particularly in areas where terrorist messages spread.
- Open-source intelligence from the internet and social media is used to track terrorist activities.
    - **Artificial intelligence and machine learning** can be used for better prediction and identification of attacks.
- Intelligence gathering must be enhanced by incorporating local insights and community participation.
    - This helps to identify radicalization and other activities at the local level.

- The National Intelligence Grid is a key initiative for enhancing intelligence gathering.

Border Security

- Border security is essential to prevent the infiltration of terrorists, weapons, and drugs.
    - India has a long and porous border with several countries, making it vulnerable.
- Border guarding forces need to be strengthened with modern technology and surveillance equipment.
    - This includes the use of **UAVs, drones, and other sensor technology**.
- A comprehensive and integrated border management system is needed to secure borders.
    - The **Comprehensive Integrated Border Management System (CIBMS)** uses non-physical barriers.
- Coordination between various agencies is necessary for effective border management.
    - The Border Security Force (BSF) is the world's largest border guarding force.
- **The concept of Village Volunteer Forces** can be promoted for better border management.
    - These forces can assist in gathering local intelligence and border security.
- The Indo-Myanmar border has become a route for drug trafficking and other illegal activities.
    - This area is also used by insurgent groups, making it difficult to maintain security.

Counter-Insurgency Operations

- Counter-insurgency operations are needed to combat both domestic and foreign terrorists.
    - These operations require the deployment of armed forces in a counter-insurgency role.
- The Armed Forces Special Powers Act (AFSPA) is used to deal with extraordinary law and order situations.
    - It is important to apply the **minimum force** required when using the AFSPA.
- Counter-insurgency operations must be conducted in a way that protects human rights.
    - Security forces should operate with accountability and transparency to avoid abuse.
- A multi-pronged strategy should address the root causes of insurgency, like development and governance.
    - This includes ensuring that the fruits of socio-economic development are inclusive.
- Coordination between the central and state governments is vital in counter-insurgency efforts.
    - This involves dialogue with insurgent groups and confidence building measures.
- The National Security Guard (NSG) is a world-class 'zero-error' force for counter-terrorism.
    - It is capable of combating any type of attack in a short amount of time.
- The Commando Battalions for Resolute Action (COBRA) are also used in counter-insurgency operations.
    - They are a specialized force for jungle warfare and combat operations.

Community Engagement & Rehabilitation

Winning Hearts and Minds, Deradicalization Programs

- Winning hearts and minds involves engaging communities to build trust and cooperation against terrorism.
    - This includes addressing grievances and ensuring inclusive development,.
- Counter narratives should be used to challenge terrorist propaganda and promote peace.
    - Emphasizing the true essence of religions can counter radicalization,.
- Deradicalization programs aim to rehabilitate and reintegrate former extremists into society.
    - These programs include counseling, education, and skill development.
- Community participation is essential for identifying and addressing factors that lead to extremism.
    - Local leaders and community-based organizations should be involved.
- Education can play a key role in creating a peaceful environment and reducing susceptibility to terrorism.

    - People must understand that the politics of war are human creations and can be changed,.
- Rehabilitation of orphans and women who are affected by terrorism is important for social welfare.
    - This would counter the recruitment of new members by terrorist groups,.

Specific Initiatives in J&K

- The roots of militancy in Jammu and Kashmir (J&K) trace back to the late 1940s with attacks from Pakistan.
    - However, the level of violence has drastically reduced in recent years,.
- Government initiatives include consensus-building by talking to all sections of political opinion.
    - Early return of statehood to J&K is seen as a long term reform,.
- The government is also focused on skill development for dropouts through the **Himayat** program.
    - The **Special Industry Initiative (SII J&K)** 'UdDAAN' is another scheme focused on jobs,.
- There is a focus on improving infrastructure in J&K through a special assistance package from the PM,.
    - A package of Rs. 80,068 crores was announced in 2015,.
- Efforts are being made to counter attempts to communalize the Kashmir valley.
    - The terror group **'The Resistance Front'** is attempting to show it as a political rather than religious cause,.
- Part-time terrorists are under the radar and are difficult to track compared to full time terrorists.
    - Use of small arms is common, transported across the border using drones.
- Long-term solutions include creating a sustainable environment of peace and development.
    - It is important to have consensus building by talking to all sections of political opinion,.
- A multi-pronged approach should be adopted to address terrorism in J&K.
    - This includes economic, social and developmental initiatives.

International Cooperation

Bilateral and Multilateral Cooperation, Treaties

- International cooperation is crucial for addressing terrorism, a transnational crime that requires collective effort.
    - This includes sharing intelligence, best practices, and coordinated action.
- Bilateral agreements with nations such as the US, Singapore, Israel, and Japan promote research and information sharing.
    - These agreements focus on cyber security and other counter-terrorism efforts.
- India uses international forums like the **UN Counter-Terrorism Committee (UNCTC)** for best practices and cooperation.
    - The Delhi Declaration (2022) also announced the same.
- **The Financial Action Task Force (FATF)** is an intergovernmental body for combating money laundering and terrorist financing.
    - It sets international standards and promotes effective implementation of measures.
- The **Vienna Convention (1988)** was a first major initiative in the fight against money laundering.
    - It aims to curb the laundering of drug money, providing measures for combating it.
- The **Council of Europe Convention (1990)** facilitates cooperation in investigations and seizures related to money laundering.
    - It also establishes a definition of money laundering and ways to combat it.
- The **Budapest Convention** is a treaty to address internet and computer crime by harmonizing laws.

    - It requires cooperation among nations, but India has not joined due to sovereignty concerns.
- The **International Convention for the Suppression of the Financing of Terrorism (1999)** is used to combat terror financing.
    - Other relevant conventions include the **UN Convention against Transnational Organized Crime (2000)**.
- **Interpol** is used to cooperate with other countries to track down terror suspects and networks.
    - It plays an important role in global efforts against money laundering and related crimes.
- International cooperation is needed to address the rapid pace of technological progress in cybercrime.
    - Cyber technologies make it difficult to detect money launderers.
- There should be a need for a security-oriented approach involving cooperation between police and intelligence agencies.
    - This helps to redress the causes that can lead to a rise in terrorist acts.
- To effectively combat terrorism, a multi-pronged approach involving the whole world is needed.
    - This would create a global environment where terrorists cannot thrive.

Concept/Subtopic	Definition/Explanation	Examples/Case Studies	Linkages/Connections	Key Points/Formulas/Theories	Practice Questions
I. Organized Crime (e.g., Drug Trafficking)	Structured criminal activity focused on illegal drug trade for profit.	* Cartel X in Mexico, Golden Crescent route. * Local examples like drug syndicates in India.	Links to: Money Laundering, corruption, funding terrorism.	- Characteristics: Hierarchical, violence, corruption. - Profit motivated.	How can drug trafficking be curbed? What are its consequences?
II. Terrorism (e.g., Religious Terrorism)	Political violence driven by religious extremism, aiming to instill fear.	* ISIS activities, * Al-Qaeda operations. *Specific attacks like 26/11.	Links to: Ideological extremism, radicalization, funding by organized crime.	- Key Motives: Political aims, religious extremism. - Use of violence as a tool.	How religious radicalization poses a threat to India's internal security? Suggest remedies.
III. Linkages (e.g., Funding)	How Drug money is used to finance terror activities.	Specific example of Afghan drug money funding Taliban.	Links to: Organized Crime, terrorism, money laundering.	- Terrorist groups use methods like hawala, money laundering etc. - Shared networks and routes.	Analyse the nexus between drug trafficking and terrorism.

IV. Counter-terrorism Measures (e.g., NMFT)	A global counter-terrorism conference aimed to curb terror financing.	* Details of the 2022 conference in New Delhi * Specific strategies adopted by members.	Links to: Financial intelligence, international cooperation, national security.	- The need for global financial intelligence sharing. - Importance of international and national financial reforms.	Evaluate the effectiveness of 'No Money for Terror' initiatives in countering terrorism.

Various Security forces and agencies and their mandate Questions: 1
Various Security forces and agencies and their mandate 1
Overview of Indian Security Apparatus 1
Brief Overview of India's Security Structure 1
Internal vs External Security Forces 1
Central Armed Police Forces (CAPFs)/ Paramilitary Forces 2
Definition: Meaning of CAPFs/Paramilitary Forces 2
CAPFs & their Mandate 3
Border Security Force (BSF) 3
Central Reserve Police Force (CRPF) 3
Indo-Tibetan Border Police (ITBP) 4
Central Industrial Security Force (CISF) 4
Sashastra Seema Bal (SSB) 4
Assam Rifles (AR) 4
National Security Guard (NSG) 5
Central Armed Police Forces (CAPFs)/ Paramilitary Forces: Role and Functions 5
Border Management 5
Internal Security Duties 5
Disaster Relief 6
VIP Security 6
Intelligence and Investigative Agencies: Central Intelligence Agencies 7
Intelligence Bureau (IB) 7
Research and Analysis Wing (RAW) 7
Investigative Agencies 7
National Investigation Agency (NIA) 7
Central Bureau of Investigation (CBI) 7
Enforcement Directorate (ED) 8
Narcotics Control Bureau (NCB) 8
Role and Mandate 8
Intelligence gathering and analysis 8
Investigation of criminal cases 8
Inter Agency Cooperation 9
Coast Guard 9
Mandate (maritime security, search and rescue, law enforcement) 9
Organizational Structure 9
Headquarters location 9
Territorial Army (TA) 10
Mandate (support to regular army, emergency tasks) 10
Eligibility to join (citizenship, age, physical fitness) 10
Incentives to members 10
National Cadet Corps (NCC) 10
Mandate (youth development, leadership training) 10
Organizational structure 10
Eligibility to join 11
Incentives to members 11

Internal Security Challenges and Role of Agencies:..... 11

Various Security forces and agencies and their mandate Questions:

- [ ] Name the para-military forces of the Government of India and their normal roles. (83/10)
- [ ] What are the internal security challenges being faced by India? Give out the role of Central Intelligence and Investigative Agencies tasked to counter such threats. (250 words) (UPSC GS 3 2023/15 marks)
- [ ] What is Territorial Army? For what reasons has it been constituted? Who are eligible to join it? What incentives are given to the members of the Territorial Army? (100 words) (81/15)
- [ ] What are the main tasks assigned to the Coast Guard Organisation? What is its setup? Where are its headquarters located? (82/10)
- [ ] Why was the National Cadet Corps established in 1948? How is the Corps organised and who are eligible to join it? Who are responsible for running the organization? What incentives are available to those, who joins the N.C.C.? (100 words) (83/20)
- [ ] What are the following and what are their functions? (i) Coast Guard (ii) Territorial Army (iii) Border Security Force (87/15)

Various Security forces and agencies and their mandate

Overview of Indian Security Apparatus

Brief Overview of India's Security Structure

- The **Cabinet Committee on Security (CCS)** is the apex body for executive action on national security matters.
    - It oversees the entire internal security apparatus.
- The **National Security Council (NSC)** considers all aspects of national security and is headed by the Prime Minister.
    - The National Security Advisor is its secretary.
- The NSC has a three-tier structure: the **Strategic Policy Group (SPG)**, **National Security Advisory Board (NSAB)**, and the **National Security Council Secretariat**.
    - The SPG is the primary forum for inter-ministerial coordination.
- The Ministry of Home Affairs (MHA) manages the operational aspects of border and internal security.
    - Coordination takes place through the Cabinet Secretariat and the Prime Minister's Office (PMO).
- **Central Armed Police Forces (CAPFs)** are under the MHA, and are deployed for internal security and border guarding.
    - These include the **Border Security Force (BSF)**, **Central Reserve Police Force (CRPF)**, and others.
- The **Central Industrial Security Force (CISF)** protects vital installations like airports and power plants.
    - It provides security to public sector undertakings and other sensitive organizations.
- The **National Security Guard (NSG)** is a specialized counter-terrorism force.
    - It is also tasked with securing high-risk VIPs.
- Intelligence agencies like the **Intelligence Bureau (IB)** and the **Research and Analysis Wing (R&AW)** gather information.
    - R&AW controls the **Special Frontier Force (SFF)**, a covert paramilitary unit.
- The **Indian Computer Emergency Response Team (CERT-In)** is responsible for cyber security.
    - It responds to computer security incidents and promotes effective IT security practices.

Internal vs External Security Forces

- Internal security forces primarily deal with threats within the country such as insurgency and terrorism.

    - The **CRPF** is a counterinsurgency force that also maintains law and order.
- The **Assam Rifles (AR)**, one of the oldest paramilitary forces, handles internal security in the North-East.
    - Its role includes counter-insurgency operations in the Indo-Myanmar border region.
- External security forces are mainly concerned with protecting the country's borders from external threats.
    - The **Border Security Force (BSF)** is the primary force for guarding international borders.
- The **Indo-Tibetan Border Police (ITBP)** is deployed along the Indo-China border.
    - It also works to prevent smuggling and other border-related crimes.
- The **Sashastra Seema Bal (SSB)** guards the borders with Nepal and Bhutan.
    - It plays a vital role in preventing cross-border crimes.
- The **Special Frontier Force (SFF)**, though a paramilitary unit, is controlled by the external intelligence agency, R&AW.
    - It is primarily composed of Tibetan exiles and Gorkhas.
- The **National Security Guard (NSG)** is a specialized force trained for counter-terrorism, and is deployed in both internal and external security.
    - It can act as sky marshals on domestic and international flights.
- The Indian Army also plays a critical role in border management and counter-insurgency operations.
    - It works in tandem with the paramilitary forces.
- The Indian Coast Guard is responsible for maritime security, safeguarding both the territorial sea and the Exclusive Economic Zone (EEZ).
    - It works to ensure the safety of shipping lanes.
- There are concerns about overlapping roles and responsibilities of the various security forces and agencies.
    - There are also questions about whether border guarding forces should be employed for counter-insurgency.

Central Armed Police Forces (CAPFs)/ Paramilitary Forces

Definition: Meaning of CAPFs/Paramilitary Forces

- **Paramilitary forces** are semi-militarized organizations with military-like structure, training, and subculture.
    - They are not part of the state's formal armed forces, and usually a light infantry group.
- **CAPFs** is a uniform nomenclature for seven security forces under the Ministry of Home Affairs (MHA).
    - These forces perform various functions such as guarding borders, and counter-terrorism.
- The seven CAPFs include the Border Security Force (BSF), Central Reserve Police Force (CRPF), and Central Industrial Security Force (CISF).
    - Also included are the Indo-Tibetan Border Police (ITBP), Sashastra Seema Bal (SSB), Assam Rifles, and National Security Guard (NSG).
- **CAPFs** are administered by the Ministry of Home Affairs and are used for maintaining internal security.
    - These forces also perform other duties like disaster management and election duties.
- **Paramilitary forces** are trained similarly to the military, and during conflict they are responsible for border protection.
    - The BSF is responsible for border protection and subordinated to the Army in duty execution.
- The term "paramilitary" is not formally defined by any government legislation or rule.
    - The term has been applied to different types of forces.
- The **Assam Rifles**, though a CAPF under MHA, is commanded by an Army officer and has dual control.

    - The recruitment, rewards, and promotion of its personnel are governed by MHA rules.
- The **Central Reserve Police Force (CRPF)** is primarily responsible for internal security and counterinsurgency operations.
    - It also assists state and union territory police forces in maintaining law and order.
- The **Border Security Force (BSF)** is responsible for guarding India's international borders.
    - It is the world's largest border guarding force, protecting both the land and sea borders.
- The **Indo-Tibetan Border Police (ITBP)** is tasked with guarding the Indo-China border and preventing smuggling.
    - It was initially raised after the 1962 Sino-Indian conflict to organize the border.
- The **Sashastra Seema Bal (SSB)** protects the Indo-Nepal and Indo-Bhutan borders.
    - It plays a vital role in preventing cross-border crimes like smuggling and human trafficking.
- The **Central Industrial Security Force (CISF)** provides security to critical infrastructure like airports and public sector units.
    - It also safeguards sensitive establishments and projects.
- The **National Security Guard (NSG)** is a specialized force trained for counter-terrorism activities.
    - It is equipped to combat any type of attack and also acts to provide close security to VIPs.

CAPFs & their Mandate

Border Security Force (BSF)

- The **BSF's primary mission** is to protect India's international land and sea borders during peace and war.
    - It is the world's largest border-guarding force with a 6,386.36-kilometer-long international border.
        - 2.7 lakh personnel, the BSF is the world's largest border guarding force.
- The BSF prevents **transnational crimes**, smuggling, and unauthorized entry into or exit from Indian territory.
    - It is responsible for border protection and is subordinated to the Army during conflict.
- BSF also played a role in preventing infiltration during the Kargil conflict in 1999.
    - The force defends the country's integrity in tandem with the Indian Army.
- The BSF is also responsible for **promoting a sense of security** among the people living near the borders.
    - It is also tasked with preventing any illegal activities from across the border.
- BSF also has jurisdiction and detention powers under the customs act and CrPC, powers currently restricted to BSF.
    - These powers could also be allotted to other CAPFs.

Central Reserve Police Force (CRPF)

- The **CRPF's main role** is to maintain internal security and assist in counter-insurgency operations.
    - It aids state and union territory police in maintaining law and order.
- The **CRPF** is the country's primary internal security force, with a strength of 3.25 lakh personnel.
    - It is recognized for its contribution to internal security.
- The CRPF is actively involved in **counter-left-wing extremism** and maintaining law and order.
    - It was in charge of guarding the India-Pakistan border until the BSF was formed.
- The **Commando Battalions for Resolute Action (COBRA)** are specialized units of the CRPF trained for jungle warfare.
    - They combat internal security threats and are capable of guerrilla warfare.

Indo-Tibetan Border Police (ITBP)

- The **ITBP** is responsible for guarding the Indo-China border and preventing border-related crimes.
    - It was founded in 1962 following the Sino-Indian conflict.
- The ITBP is tasked with keeping an eye on **illegal immigration and trans-border smuggling**.
    - The force was deployed to guard the entire India-China border in 2004.
- The **ITBP provides security** to various sensitive installations of national importance.
    - These include the Rumtek Monastery (Sikkim) and the Lal Bahadur Shastri National Academy.
- The Cabinet Committee on Security (CCS) recently approved raising seven new ITBP battalions.
    - This will give a major push to counter Chinese maneuvers at the border.
- The ITBP is currently engaged in a standoff with the Chinese PLA in eastern Ladakh.
    - The Indian Army has pushed for operational control over ITBP.

Central Industrial Security Force (CISF)

- The **CISF provides security** and protection to vital installations of national/strategic importance.
    - This includes Public Sector Undertakings (PSUs), airports, and atomic power plants.
- The **CISF** also secures space organizations, industrial units, and important national museums.
    - It also guards government buildings in Delhi and other sensitive organizations.
- The **CISF** safeguards critical infrastructure including airports and other public-sector projects.
    - It also secures important government buildings.
- With around 165,000 personnel, the **CISF** is the world's largest industrial security force.
    - Its mandate is to provide specialized security to sensitive sectors.

Sashastra Seema Bal (SSB)

- The **SSB** is primarily responsible for guarding the Indo-Nepal and Indo-Bhutan borders.
    - It was founded in 1963, protecting 2450 km of borders.
- The **SSB** plays a key role in preventing cross-border crimes and anti-national activities.
    - It is crucial in preventing smuggling, and human trafficking.
- **SSB** is also engaged in counter-insurgency operations and internal security duties.
    - It performs election duties and law and order duties in various parts of India.
- The **SSB** is a border guarding force that also contributes to internal security.
    - It is essential in maintaining security along open borders.

Assam Rifles (AR)

- The **Assam Rifles (AR)** is the oldest paramilitary force, established in 1835.
    - Its initial purpose was to protect British tea estates from tribal raids.
- The **Assam Rifles** is tasked with maintaining law and order in the North-Eastern areas of India.
    - It is also involved in counter-insurgency operations in the region.
- The **AR** has a dual control structure, with administrative control under the MHA and operational control with the Indian Army.
    - Its personnel are governed by MHA rules for recruitment, rewards, and promotion.
- **Assam Rifles** also took part in conventional combat during the 1962 Sino-India War.
    - It operated as part of the Indian Peace Keeping Force (IPKF) in Sri Lanka in 1987.
- The **Assam Rifles** is a CAPF but is manned by Army personnel and officers.
    - It is tasked with ensuring border security in India's north-eastern regions.
- The **Assam Rifles** has a unique role, guarding borders while also conducting counter-insurgency.

    - There are differing views on whether it should be employed on counter-insurgency or guarding borders.

National Security Guard (NSG)

- The **NSG** is a specialized strike force for counter-terrorism and anti-hijacking operations.
    - It was raised in 1984 to combat terrorism.
- The **NSG** is also entrusted with securing high-risk VIPs and acts as sky marshals.
    - It provides close protection to designated protectees.
- **NSG Commandos** are trained for high-risk tasks like counter-terrorism and bomb disposal operations.
    - They are experts in neutralizing terrorist threats and handling hijack situations.
- The **NSG** is a unique blend of personnel from the Army, CAPFs, and State Police Forces.
    - It has gained a reputation for excellence due to its training standards and operational efficiency.
- The **NSG** has established regional hubs to reduce response times and ensure a pan-India presence.
    - There are five hubs in Mumbai, Chennai, Hyderabad, Kolkata and Gandhinagar.
- The **NSG**, also known as 'Black Cats,' has conducted many successful counter-terrorist operations.
    - It is capable of combating any type of attack in a very short time.

Central Armed Police Forces (CAPFs)/ Paramilitary Forces: Role and Functions

Border Management

- **CAPFs** play a vital role in guarding India's extensive land and maritime borders, ensuring national security.
    - They prevent cross-border crimes like smuggling, illegal immigration, and human trafficking.
- **Border management** involves coordinating actions between various agencies for securing the frontiers.
    - This includes administrative, diplomatic, security, intelligence, and economic agencies.
- **BSF** is primarily responsible for protecting India's international borders during both peace and war.
    - It is the world's largest border guarding force, covering 6,386.36 km of international border.
- The **SSB** is tasked with guarding the Indo-Nepal and Indo-Bhutan borders.
    - It was founded in 1963 and is responsible for protecting 2450 km of borders.
- The **ITBP** is responsible for guarding the Indo-China border, preventing illegal activities.
    - It was formed in 1962 following the Sino-Indian conflict.
- **Border management** includes using technology like UAVs and surveillance for effective control.
    - It is necessary to ensure forces maintain minimum strength at all times.
- The government has approved the construction of 422 Composite Border Outposts (BOPs).
    - 326 of these are to be built along the Indo-Bangladesh border.
- **Comprehensive Integrated Border Management System (CIBMS)** uses non-physical barriers where fencing is not possible.
    - This system uses technology as a force multiplier.
- The **concept of Village Volunteer Forces (VVFs)** has been successful in border management.
    - India should promote this concept further in border areas.

Internal Security Duties

- **CAPFs** are crucial in maintaining internal security and dealing with insurgency and terrorism.
    - They assist state police forces in maintaining law and order.

- The **CRPF** is a key force for internal security and counter-insurgency operations.
    - It is actively involved in counter-left-wing extremism operations.
- **COBRA**, a specialized unit of the CRPF, is trained for jungle warfare.
    - This unit combats internal security threats through guerilla warfare.
- The **Assam Rifles (AR)** has a dual role, maintaining border security and internal security.
    - It operates in the North-East and conducts counter-insurgency operations.
- The **NSG** is a specialized force for counter-terrorism and anti-hijacking operations.
    - It is trained for high-risk tasks such as bomb disposal and hostage situations.
- **CAPFs** are deployed during elections to ensure a safe and secure environment.
    - They play a vital role in maintaining law and order during such events.
- **CAPFs** also assist in maintaining public order during festivals, protests and other such events.
    - Their deployment helps maintain peace and stability during sensitive situations.
- **CAPFs** help in managing internal conflicts, often in unconventional and ambiguous modes.
    - These forces are trained to deal with asymmetrical conflicts that are not conventional.
- **AFSPA** is a tool to deal with extraordinary law and order situations perpetrated by insurgents.
    - It allows the armed forces to be deployed in counter-insurgency roles.

Disaster Relief

- **CAPFs** provide immediate relief during natural disasters and other emergencies.
    - They assist in search and rescue operations and provide aid to affected populations.
- The **BSF** plays a crucial role in rescue and traffic control operations during civil emergencies.
    - It also provides medical assistance and shelter during disasters.
- **ITBP** is also trained to carry out rescue operations and provide relief during natural calamities.
    - Its personnel are deployed in disaster prone areas for rapid response.
- **CRPF** provides assistance during natural disasters, supplementing efforts by civil authorities.
    - They are involved in evacuation, setting up temporary shelters and distributing aid.
- **CAPFs** also play an important role in providing immediate support and relief to people during emergencies.
    - These forces are trained to provide necessary resources during such times.
- **CAPFs** are often the first responders during any natural disaster because of their reach.
    - Their personnel are trained to operate in the toughest and most demanding conditions.

VIP Security

- **CAPFs** are entrusted with providing security to high-risk VIPs.
    - They provide close protection to designated individuals who are under security threat.
- The **NSG** is responsible for providing close protection to high-risk VIPs.
    - They are experts in securing designated individuals and preventing any security threat.
- The **CISF** also secures sensitive government buildings and protect important personnel.
    - They also protect various public sector undertakings and national assets.
- The **CRPF** also engages in security for VIPs as part of their duties.
    - They are deployed to provide security at places where VIPs are visiting.
- **CAPFs** are tasked with providing a secure environment for high-profile individuals.
    - They conduct regular security drills and protocols for high-value assets and people.
- **CAPFs** also guard the installations which are of national strategic importance.
    - They are responsible for maintaining the safety and security of these installations.

Intelligence and Investigative Agencies: Central Intelligence Agencies

Intelligence Bureau (IB)

- The **Intelligence Bureau** was responsible for raising the **Special Frontier Force (SFF)** after the 1962 China-India war.
    - The SFF was initially comprised of Tibetan exiles.
- The Intelligence Bureau chief is a member of the **National Security Council (NSC)**.
    - The NSC considers all aspects of national security.
- The **IB** is responsible for internal intelligence gathering, counter-intelligence, and counter-terrorism within India.
    - The IB plays a crucial role in identifying and countering threats to internal security.
- The IB works to **counter subversive activities** by non-state actors using internet and social media.
    - It identifies digital security attacks and breaches using AI and machine learning.
- The **IB** is involved in border management and coordinates with various agencies.
    - It helps secure borders against hostile interests and facilitate legitimate trade.

Research and Analysis Wing (RAW)

- The **Research and Analysis Wing (R&AW)** is India's external intelligence agency.
    - The R&AW controls the **Special Frontier Force (SFF)**.
- The **R&AW** gathers intelligence from outside India.
- It is focused on external threats to national security and strategic interests.
- The **R&AW** plays a crucial role in counter-terrorism by monitoring international terrorist organizations.
    - It tracks terrorist activities and their funding sources.
- The **R&AW** works to secure India's interests, including border security and maritime security.
    - It helps maintain security with various security and intelligence initiatives.
- The **R&AW** contributes to the development of a national security strategy.
- The Defence Planning Committee works to create a draft national security strategy.

Investigative Agencies

National Investigation Agency (NIA)

- The **National Investigation Agency (NIA)** is a central agency to investigate offenses affecting the sovereignty, security and integrity of India.
    - The NIA has been created to strengthen the fight against terror.
- The **NIA** can take up cases from state governments for investigation of scheduled offenses.
    - State governments must extend full assistance to the NIA.
- The Central government can direct **NIA** to take over a case if it believes a scheduled offense has been committed.
    - The NIA has the power to suo moto cognisance of such cases.
- The **NIA** is involved in counter-terrorism efforts and investigates terror financing and organized crime.
    - The NIA is considered to be a positive step in dealing with such issues.

Central Bureau of Investigation (CBI)

- The **Central Bureau of Investigation (CBI)** is India's premier investigating police agency.
    - The CBI investigates corruption, economic offenses and other serious crimes.
- The **CBI** works with other agencies to counter money laundering and related crimes.
    - The CBI investigates cases of money laundering separately from other scheduled offenses.
- The **CBI** coordinates with national and international intelligence agencies.
    - The CBI strengthens efforts against money laundering and related crimes.

Enforcement Directorate (ED)

- The **Enforcement Directorate (ED)** is an Indian law enforcement agency focused on economic crimes.
    - The ED is tasked with enforcing economic laws and combatting illegal acts.
- The **ED** investigates money laundering offenses under the Prevention of Money Laundering Act (PMLA).
    - The ED has the power to seize property if it is proven to be proceeds of crime.
- The **ED** works with the Financial Intelligence Unit-India (FIU-IND) to investigate financial crimes.
    - The FIU-IND provides the ED with information related to suspect transactions.

Narcotics Control Bureau (NCB)

- The **Narcotics Control Bureau (NCB)** is India's apex agency for combating drug trafficking.
    - The NCB aims to cut off drug supplies and prevent drug abuse.
- The **NCB** is involved in the seizure and destruction of illicit drugs.
    - The NCB also works to coordinate international efforts against drug trafficking.
- The **NCB** coordinates with other agencies to counter drug trafficking, gunrunning, and money laundering.
    - Drug cartels and other criminal organizations are increasingly intertwined
- The **NCB** combats drug trafficking which is linked to terror financing, gunrunning, and human trafficking.
    - India is located near the two largest opium-growing regions of the world.

Role and Mandate

Intelligence gathering and analysis

- The **Intelligence Bureau (IB)** gathers internal intelligence and counters threats within India.
    - The IB works to counter subversive activities using social media and the internet.
- The **Research and Analysis Wing (R&AW)** gathers external intelligence related to national security.
    - The R&AW monitors international terrorist organizations and their activities.
- The **National Security Advisory Board (NSAB)** undertakes long-term analysis of national security issues.
    - The NSAB gives perspectives on national security issues to the NSC.
- **Financial Intelligence Unit-India (FIU-IND)** gathers information on suspect financial transactions.
    - The FIU-IND provides information to the ED for investigating financial crimes.

Investigation of criminal cases

- The **National Investigation Agency (NIA)** investigates offenses that threaten India's security.
    - The NIA investigates terror financing and organized crime, and can take suo moto cognisance.
- The **Central Bureau of Investigation (CBI)** investigates corruption, economic offenses, and serious crimes.
    - The CBI coordinates with other agencies to counter money laundering.
- The **Enforcement Directorate (ED)** investigates money laundering under the PMLA.
    - The ED can seize property if it is the result of a scheduled offense.
- The **Narcotics Control Bureau (NCB)** combats drug trafficking and abuse.
    - The NCB coordinates with international agencies to counter drug trafficking.
- **Cybersecurity** is critical in investigating cybercrimes and digital security breaches.
    - CERT-In is responsible for responding to cyber security incidents.

Inter Agency Cooperation

- The **Strategic Policy Group (SPG)** is the primary forum for coordination and integration of inputs.
    - The SPG is chaired by the Cabinet Secretary.
- The **National Security Council (NSC)** is the apex body that deliberates on all aspects of national security.
    - The NSC includes the Prime Minister and several ministers.
- Intelligence and investigative agencies cooperate to counter internal and external threats.
    - Agencies such as the IB, R&AW, NIA, CBI, ED, and NCB work together.
- Border management requires coordination among administrative, security, and intelligence agencies.
    - Village Volunteer Forces (VVFs) also help in border management.
- **International cooperation** is essential for addressing transnational crimes like terrorism, drug trafficking, and money laundering.
    - India is a member of Financial Action Task Force (FATF).

Coast Guard

Mandate (maritime security, search and rescue, law enforcement)

- The **Indian Coast Guard (ICG)** is responsible for maritime security and protecting offshore resources.
    - The ICG was formally established under the Coast Guard Act, 1978.
- The **ICG** assists mariners in distress, and enforces maritime laws against poaching, smuggling, and narcotics.
    - The ICG's responsibilities include the protection of the Exclusive Economic Zone (EEZ).
- The **ICG** is mandated to protect the coast and offshore areas including oil, fish and minerals.
    - The ICG also enforces maritime laws with respect to sea poaching, smuggling and narcotics.
- The **ICG** is tasked to preserve marine environment and ecology, and protect rare species.
    - The ICG also collects scientific data and backs up the navy during war.
- The **ICG** conducts real-time coastal monitoring and surveillance with a network of static sensors.
    - The ICG has established 46 radars for this coastal surveillance network (CSN).
- The **ICG** works to ensure the safety and security of shipping lanes, especially choke points.
    - These choke points include the Strait of Hormuz, Bab-el-Mandeb, and Strait of Malacca.

Organizational Structure

- The **Indian Coast Guard** is a multi-mission agency that conducts year-round real-life maritime operations.
    - The ICG has a wide range of tasks both for surface and air operations.
- The **ICG** is headed by the Director General Indian Coast Guard (DGICG) based at Coast Guard Headquarters.
    - The DGICG commands and supervises all activities of the ICG.
- The **Indian Coast Guard** is a part of the unified maritime command led by the Indian Navy.
- This unified command ensures integrated maritime security.
- The **National Maritime Security Coordinator (NMSC)** coordinates with the ICG and other maritime agencies.
    - The NMSC is appointed under the National Security Advisor.
    - The NMSC liaises with coastal states and other maritime security agencies.

Headquarters location

- The **Coast Guard Headquarters (CGHQ)** is located in New Delhi.
    - The DGICG, who leads the ICG, is based in New Delhi.

Territorial Army (TA)

Mandate (support to regular army, emergency tasks)

- The **Territorial Army (TA)** is an organization of volunteers who receive military training.
    - The TA provides support to the regular army in times of emergency.
- The **TA** assists in maintaining essential services and natural disaster relief.
    - The TA helps in situations where civil administration requires military support.
- The **TA** is responsible for assisting the civil authorities in maintaining law and order.
    - The TA assists during internal disturbances and security threats.
- The **TA** is also tasked to protect vulnerable installations and lines of communication.
    - This protection is during times of conflict or natural disasters.

Eligibility to join (citizenship, age, physical fitness)

- Indian citizens, both male and female, between 18 to 42 years, can join the TA.
    - Candidates must meet the required standards of physical and medical fitness.
- **Ex-servicemen** can also join the TA.
    - Ex-servicemen can join the TA with relaxed age limits.
- Candidates must meet the specific eligibility criteria for the TA, such as physical fitness.
    - Applicants must fulfill all requirements as per the TA regulations.
- The **TA** is open to employed people who can serve without disrupting their primary occupation.
    - The TA is a part-time commitment with annual training camps.

Incentives to members

- TA members receive annual training and honorarium allowances.
    - TA members get certain pay and allowances while on duty or training.
- TA members are provided with opportunities to serve the nation without quitting their primary job.
    - TA members serve in uniform but remain civilians most of the year.
- TA service counts towards pension and other benefits in many government services.
    - TA service can improve the career prospects of members in specific government jobs.
- The **TA** also provides a platform for citizens to contribute to national security.
    - The TA helps in creating a sense of national pride and responsibility.

National Cadet Corps (NCC)

Mandate (youth development, leadership training)

- The **National Cadet Corps (NCC)** aims to develop character, comradeship, discipline, and leadership in youth.
    - The NCC provides opportunities to motivate youth to join the armed forces.
- The **NCC** is a youth development movement with military training to create a sense of patriotism.
    - The NCC seeks to create a human resource of organized and motivated youth.
- The **NCC** conducts activities that promote national integration and social awareness.
    - NCC cadets are trained to become responsible citizens and good leaders.
- The **NCC** provides basic military training and leadership skills to students in schools and colleges.
    - NCC training includes drills, weapon training, adventure activities and community development.

Organizational structure

- The **NCC** is a tri-services organization, comprising the Army, Navy, and Air Force wings.
    - The NCC is headed by a Director General (DG) at the national level.
- The **NCC** has units in schools and colleges, under the command of commissioned officers.
    - The NCC directorate is responsible for the administration of the corps in states.
- The **NCC** curriculum includes training and activities that are overseen by commissioned officers.
    - The NCC training also involves participation in camps and adventure activities.

- The **NCC** is part of the Ministry of Defence and is staffed by officers from the armed forces.
    - The NCC works closely with the armed forces to train young cadets.

Eligibility to join

- Students from schools and colleges are eligible to enroll in the **NCC**.
    - The eligibility criteria include age limits and physical fitness requirements.
- The **NCC** is open to both boys and girls.
    - NCC enrollments can happen at junior and senior levels.
- Applicants must meet the specific eligibility criteria for the NCC, such as physical fitness.
    - Applicants must fulfill all requirements as per the NCC regulations.

Incentives to members

- **NCC** cadets get preference in selection for the armed forces and other uniformed services.
    - Vacancies in the Indian Army are reserved for NCC cadets.
- **NCC** cadets also receive preference in recruitment to various government jobs.
    - The NCC helps in developing discipline and leadership qualities.
- **NCC** 'C' certificate holders get additional weightage during SSB interviews.
    - The 'C' certificate is an important incentive for NCC cadets.
- **NCC** cadets are encouraged to participate in adventure activities and community development.
    - Cadets also get opportunities to represent their unit at national events.

Internal Security Challenges and Role of Agencies:

A. Major internal security threats in India: (Read it from the notes)
B. Roles of various agencies in combating the above challenges. (Read it from the notes)

Mains-Level Note-Making Table: Security Forces & Agencies

Force /Agency	**Abbreviation**	**Mandate/Role (Detailed)**	**Organizational Structure (Key Elements)**	**Specific Functions & Area of Operations**	**Challenges Faced**	**Recent Developments/Initiatives**	**Inter-Agency Coordination (with whom/how)**	**Recommendations/Reforms**	**Case Study/ Examples**
Border Security Force	BSF	*Detailed description of border guarding, preventing cross-border crimes like smuggling,	*Command structure, DG-level, divisions, specific units. Deployment strategy.*	*Specific border management, operations, use of technology like thermal imaging.* Speci	*Porous borders, difficult terrain, lack of resources. Corruption, political pressure.* Cross-	*Use of drones, new surveillance systems.* Modernization of weapons.*	*Coordination with Army, State Police. Intelligence sharing with RAW/IB.*	*Border fencing, improved intelligence. Community policing. Technology upgradation.*	*Specific instances of border management successes or failures, infiltration attempts.*

		infiltration, etc. *Specific mandate variations based on border type.		fic areas of deployment - Indo-Pak, Indo-Bangla.*	border terrorism, smuggling.*				
Central Reserve Police Force	CRPF	*Internal security roles, maintaining law & order, anti-insurgency. Specific functions based on region.*	*Command structure, different battalions, specialized units like RAF. Deployment strategy.*	*Counter-insurgency operations, riot contrl. Election duties. VIP security. Deployment in Naxal areas, Kashmir.*	*Dealing with multiple internal threats. Coordination with state police. Lack of trained manpower. Use of excess force, human rights issues.*	*Increased use of technology, new training programs. Efforts to improve image, community relations.*	*Coordination with State Police, Intelligence agencies, central agencies.*	*Better training for riot control. Local community involvement. Human Rights sensitization.*	*Specific cases of CRPF involvement in quelling riots, anti-insurgency.*

Intelligence Bureau	IB	*Detailed scope of internal intelligence gathering, analysis, counter-intelligence.* * Specific areas of focus. *	*Organizational hierarchy, divisions, units. Recruitment, training.*	*Collection and analysis of data, counter-intelligence operations. Specific cases.*	*Data gathering on sensitive issues, ensuring national security. Lack of manpower. Political interference, data leakage issues.*	*Use of data analytics, cyber intelligence.*	*Coordination with State Intelligence, Central Agencies.*	*Data Security enhancement. Political autonomy.*	*Specific cases where the intelligence agencies helped foil a terror attack.*
Research & Analysis Wing	RAW	*Detailed mandate of external intelligence gathering, analysis, strategic operations.*	*Organizational structure, hierarchy, divisions, units. Recruitment and training.*	*Gathering intelligence, counter intelligence, strategic operations Overseas operations.*	*Challenges faced in different geopolitical scenarios. Maintaining secrecy of operations.*	*Use of new technologies for communication, intelligence gathering.*	*Coordination with intelligence agencies of friendly nations.*	*Use of technology. Increase in staff strength.*	*Specific instances of external intelligence gathering leading to national security.*
National Investigation Agency	NIA	*Detailed mandate to investigate terror-*	*Organizational Structure, hierarchy,*	*Investigation of terror attacks, tracki*	*Cross border links, lack of coope*	*More powers to NIA.*	*Coordination with central and state police*	*Fast tracking trials. Coordination with central and state agencies.*	*Specific terror cases investigated by NIA.*

		related cases.	*divisions.*	*ng finances, prosecuting terrorists.*	*ration from other countries. Proving terror linkages.*		*forces. Interpol.*		
Central Bureau of Investigation	CBI	*Detailed mandate to investigate corruption, white collar crimes and major criminal cases*	*Organization structure, divisions, units.*	*Investigation of corruption at high levels, financial scams*	*Political pressure, lack of adequate personnel, long delays in investigations.*	*Modernization of investigation techniques.*	*Coordination with state police.*	*Autonomy from political interference.*	*Specific high-profile cases investigated by CBI.*