



PRAYAAS
INSTITUTE OF  EXCELLENCE



INTERNAL SECURITY

GENERAL STUDIES - 3

Class Notes

UPSC MAINS



© Prayaas Institute Pvt.Ltd.
All rights reserved.

Published by
Prayaas Institute Pvt. Ltd.

Ramashree, Near Muralidhar Veg.
No. 279, N. C. Kelkar Road,
Narayan Peth, Pune - 30
+ 91 9894998421
www.prayaas.in

UPSC MAINS

INTERNAL SECURITY
GENERAL STUDIES - 3
(Class Notes)

Year 2024 - 25

INDEX

- 1. LINKAGES BETWEEN DEVELOPMENT AND SPREAD OF EXTREMISM 1**
- 2. ROLE OF EXTERNAL STATE AND NON-STATE ACTORS IN CREATING CHALLENGES TO INTERNAL SECURITY 9**
- 3. CHALLENGES TO INTERNAL SECURITY THROUGH COMMUNICATION NETWORKS, ROLE OF MEDIA AND SOCIAL NETWORKING SITES IN INTERNAL SECURITY CHALLENGES 12**
- 4. BASICS OF CYBER SECURITY 17**
- 5. MONEY-LAUNDERING AND ITS PREVENTION 24**
- 6. SECURITY CHALLENGES AND THEIR MANAGEMENT IN BORDER AREAS 30**
- 7. LINKAGES OF ORGANIZED CRIME WITH TERRORISM 36**
- 8. VARIOUS SECURITY FORCES, AGENCIES AND THEIR MANDATE 43**

Linkages Between Development And Spread Of Extremism

First of all let us see the past year UPSC questions and understand their demand.

Questions	Keyword/Context/Demand
Article 244 of the Indian Constitution relates to administration of scheduled areas and tribal areas. Analyse impact of non-implementation of the provisions of the Fifth schedule on the growth of Left Wing extremism. (2013, 10 Marks)	Fifth schedule, Growth of Left wing extremism(LWE)
The persisting drives of the Government for development of large industries in backward areas have resulted in isolating the tribal population and the farmers who face multiple displacements. With Malkangiri and Naxalbari foci, discuss the corrective strategies needed to win the Left Wing Extremism (LWE) doctrine that affected citizens back into the mainstream of social and economic growth. (2015, 12.5 Marks)	Development, displacement and Rise of Left wing Extremism, Strategies to tackle LWE
The North-Eastern region of India has been infested with insurgency for a very long time. Analyze the major reasons for the survival of armed insurgency in this region. (2017, 10 Marks)	North East insurgency
Left Wing Extremism (LWE) is showing a downward trend, but still affects many parts of the country. Briefly explain the Government of India's approach to counter the challenges posed by LWE. (2018, 10 Marks)	LWE and government approaches to counter the same
What are the determinants of left-wing extremism in Eastern part of India? What strategy should the Government of India, civil administration and security forces adopt to counter the threat in the affected areas? (2018, 15 Marks)	Determinants of left-wing extremism in Eastern part of India, strategies for countering the same
Naxalism is a social, economic and developmental issue manifesting as a violent internal security threat. In this context, discuss the emerging issues and suggest a multilayered strategy to tackle the menace of Naxalism. (2022, 15 marks)	Naxalism as Social, Economic and developmental issue, Emerging threat from Naxalism, Multilayered strategy to tackle Naxalism

Introduction

Generally People are drawn to violence and extremism by their perceptions of injustice, misgovernance, and failure system to reach upto them. In the Indian context, due wider diversity of country there persist wider interest of different groups. Sometime these wider interest conflict with each other and also conflicts with state. The same conflict gave birth to extremism.

What is meant by Extremism??

Extremism is essentially a political term that determines the activities that are not in accordance with norms of the state, are fully intolerant towards others, reject democracy as means of governance and other way of problem solving and also rejecting existing social order.

Objectives of extremism

- To rectify the wrong doings of history.
- To seek political or social mileage for their cause.
- To bring the issues for the larger public debate.
- It also aims at recognising the identities of groups or communities by the political apparatus.
- It also aims at realising the national freedom

Types

In india extremism like

- 1. Left-wing extremism (LWE) or Naxal insurgency.**
- 2. North East insurgency**

are two prominent extremism threat to national security both of these extremism are directly connected to the development process.

- 1. Left-wing extremism (LWE) or Naxal insurgency.**

Beginning and development of LWE

- The so-called agrarian revolution began in West Bengal in 1967 when an extremist breakaway faction of the CPM began the agitation.
- The initial outburst was by groups occupying vacant lands in Naxalbari, Khoribari, and Phansidewaon, claiming that the lands were in excess of the permissible ceiling on land holdings or that they were supposed to have vested in the government, which the latter never bothered to distribute to landless and marginal farmers as provided for in the West Bengal Estate Acquisition Act of 1953 and other laws.
- The first wave of the Naxalbari region's Left Extremist movement was efficiently suppressed without much bloodshed and in a very short period of time.
- The All India Coordination Committee of Communist Revolutionaries (AICCCR) was formed in May 1968 to carry on the militant movement in various sections of India.
- In April of 1969, the CPI, a new Marxist-Leninist party, was founded (ML).

- Overt acts of violence in the name of 'class destruction' began to emerge in areas of states such as West Bengal, Andhra Pradesh, Kerala, Bihar, and Uttar Pradesh, as well as Orissa, Madhya Pradesh, and Punjab.
- These are later known as Red corridor area which are most affected by Left wing extremism or Naxalism.

Major Naxal incident in india

- **Naxalites Attack in Chattisgarh (2007)**

Naxalites attacked a police outpost, killing 55 policemen belonged to the state police and other Special Police Officers in Chhattisgarh's Rani Bodi village.

- **Naxalites Attempted Derailment (2010)**

Couple of times in the year of 2010 Naxalites attempted derailment of Triveni express and Kolkata–Mumbai mail. Kolkata Mumbai train derailment killed at least 150 persons.

- **Naxalite Attack in Dantewada (2010)**

Naxalite Rebels killed 76 persons including paramilitary personnel of the CRPF and two policemen. The series of attacks on security convoys in Dantewada district.

- **Naxal Attack in Sukma (2013)**

The 2013 Naxal attack in Darbha valley in the Sukma district of Chhattisgarh caused at least 27 deaths, including the former state ministers.

- **Sukma, Chhattisgarh 2014**

Maoists killed 14 CRPF personnel, including two officers, in Sukma. The ambush took place near Kasalpara village. There were reports of six Maoists being killed in the encounter.

- **Sukma District 2020**

17 security personnel of Chhattisgarh Police were killed in a Maoist ambush in Sukma district's Almasguda forest, including 12 from the District Reserve Guards and 5 others from Special Task Force during a security operation launched against Maoists alongside the CRPF. 15 personnel were wounded and 16 weapons stolen.

Factors responsible for spread LWE or Naxal insurgency.

- **Discontent with the government among tribal peoples**

- Loss of livelihood due to forest policy.
- Massive tribal population displacement in Naxalism-affected states as a result of development projects, mining operations, and other factors.

- **Economic factors:**

- Unemployment, poverty, a lack of health care, a lack of education and awareness, a lack of access to electricity, internet connectivity.
- The wealth divide between affluent and poor is widening.

- **Deficiency in governance:**
 - Absence of Regular administration in remote locations
 - Lack of state government measures to address the problem, poor implementation, and mishandling of government schemes.
- **Social oppression**
 - social discrimination faced by the Dalits and other lower cast OBC
 - This social discrimination creates feeling of alienation.
- **Land alienation**
 - Increased marginal landholdings.
 - Weak land reforms which lead to insecurity and exploitation of tenants.
- **Delayed process of adjudication**
 - slow judicial system.
 - The same slow system which creates frustration which ends up with illegal extremist mind framework.
- **Rehabilitation**
 - Tribal people who displaced due to development project not rehabilitated properly
 - This causes people to experience multidimensional trauma, which has major repercussions.
- **Common property resources (CPR)**
 - CPR includes such as community pasture, watershed drainages, village tanks etc. These CRR are sustainable to local communities.
 - But due to industrialisation, privatisation and development projects, the CPRs area is shrinking and govt. never look in to this matter.
- **Environment degradation**
 - Mineral extraction, deforestation creating problems like land degradation
 - These environmental problems push already vulnerable people more towards poverty.

Steps taken by Government to counter LWE

- **GreyHound Police**
commando force of Andhra Pradesh created to counter left-wing extremism.
- **Bastariya Battalion**
The Bastariya Battalion is a unit of India's Central Reserve Police Force, based in Chhattisgarh. The unit is tasked with curbing Naxalist activities in Chhattisgarh state

- **Operation Green Hunt**

Operation Green Hunt is the name used by the Indian media to describe the "all-out offensive by paramilitary forces and the states forces" against the Naxalites.

- **Special Central Assistance (SCA) for most LWE affected districts**

This Scheme was approved in 2017 and is being implemented as a sub-scheme of the Umbrella Scheme 'Modernization of Police Forces'.

- **Civic Action Programme (CAP)**

This Scheme is being implemented to bridge the gaps between Security Forces and local people through personal interaction and bring the human face of SFs before the local population.

- **Road Connectivity Project for LWE affected areas (RCPLWE)**

The Government approved this scheme for further improving road connectivity in LWE affected States, with an estimated expenditure on Rs. 11,725 Crore. Under the scheme 12081 km of roads and 593 bridges are sanctioned.

- **SAMADHAN doctrine**

It is the one-stop solution for the LWE problem. It encompasses the entire strategy of government from short-term policy to long-term policy formulated at different levels. SAMADHAN stands for-

S - Smart Leadership.

A - Aggressive Strategy,

M - Motivation and Training,

A - Actionable Intelligence,

D - Dashboard Based KPIs (Key Performance Indicators) and KRAs (Key Result Areas),

H - Harnessing Technology,

A - Action plan for each Theatre,

N - No access to Financing

- **Aspirational District**

The Ministry of Home Affairs has been tasked with the monitoring of Aspirational districts programme in 35 LWE affected districts.

2. North East insurgency

Introduction

- Insurgency is another example of development and extremism being related. The partition of India turned the North-East region into a landlocked region and affected it developmentally and economically.
- The region shares an international border of 5,182 km, with the neighbouring countries.
- The North East as a whole is not a single entity with a common political identity. Instead, it comprises many other tribes, each with their vision of their political future.

- Post-independence, the history of this region has been marred with bloodshed, tribal feuds and under development.

The state-wise of insurgent group in North-East

State	Insurgent Group
Assam	<ul style="list-style-type: none"> • ULFA (1990-present) The United Liberation Front of Assam was formed in April 1979 to establish a sovereign state of Assam for the indigenous people of Assam through an armed struggle. • KLO (1995-present) The objective of the Kamtapur Liberation Organisation (KLO) is to carve out a separate Kamtapur Nation • MULTA (1996-present) The objective of the Muslim United Liberation Tigers of Assam (MULTA) is to establish an Islamic state in India under sharia law.
Meghalaya	<ul style="list-style-type: none"> • Hynniewtre National Liberation Council It is a militant organization operating in Meghalaya. It claims to represent the Khasi-Jaintia tribal people, and its aim is to free Meghalaya from the alleged domination of outsiders (the "Dkhars") from the Indian mainland. It
Mizoram	<ul style="list-style-type: none"> • MNF insurgency (1966-1986) Mizoram's tensions were largely due to the simmering Assamese domination and the neglect of the Mizo people. In 1986, the Mizo accord ended the main secessionist movement led by the Mizo National Front, bringing peace to the region.
Manipur	<ul style="list-style-type: none"> • The first separatist faction, known as United National Liberation Front (UNLF), was founded on 24 November 1964 in Manipur. • Between 1977 and 1980, <ol style="list-style-type: none"> 1. People's Liberation Army of Manipur (PLA) 2. People's Revolutionary Party of Kangleipak (PREPAK) 3. Kangleipak Communist Party (KCP)
Nagaland	<ul style="list-style-type: none"> • NSCN insurgency (1980-present) The National Socialist Council of Nagaland was formed in 1980 to establish Greater Nagaland, encompassing parts of Manipur, Nagaland, and the north Cachar hills (Assam). The NSCN split in 1988 to form two groups, NSCN(IM) and NSCN(K).
Tripura	<ul style="list-style-type: none"> • The National Liberation Front of Tripura It was formed in March 1989. During the period 1992 to 2001, a total of 764 civilians and 184 members of the security forces were killed in NLFT attacks. In 2019, it signed the Tripura Peace Accord to end the insurgency.
Arunachal Pradesh	Arunachal Pradesh has not witnessed much insurgency. But some insurgents from Nagaland To Assam take shelter on Arunachal Pradesh land.
Sikkim	Unlike the turbulent sister-states, Sikkim was always a peaceful state since its incorporation in India

In North East each state has their unique problem but as a exam point of view we here only looking into common factors which are responsible for insurgency in North East.

Factors responsible for insurgency in the North East.

- **Historical reasons for the conflict**

Historical connections among tribes are largely Tibeto-Burman/Mongoloid (Ethnically, linguistically & culturally very distinct.)

- **Physiographic constraints** Mountain terrains make it difficult for security forces to track borders.

- **Porous borders & arms availability**

Result in arms & drugs trafficking (Golden Triangle), illegal immigration.

- **Role of state actors**

Existence of external help from Bangladesh, China and Myanmar has perpetuated the insurgencies.

- **Lack of Development**

The continuous lack of economic opportunities creates incentives for unemployed youths to join armed movements where they earn a salary.

- **Low Governance**

Issues of infrastructure, poor service delivery and lack of connectivity has been major problems in governance. All these further created problems of insurgency.

- **Sense of Alienation**

people of States in the North East have a sense of alienation that the Government of India was not paying enough attention to their development. It was this sense that had misled a few to take up arms, also one reason for insurgency in the North East.

Steps taken by Government to counter N-E insurgency

- **AFSPA**

Armed Forces (Special Powers) Act (AFSPA), 1958 is an act of the Parliament of India that grants special powers to the Indian Armed Forces to maintain public order in "disturbed areas"

- **Cutting off external support**

Improved security relationship with Myanmar and Bangladesh have cut off these supports.

- **Engagement and talks**

A lot of insurgent groups were engaged in talks due to which the violent incidents declined

over the last few years.eg:Mizo accord,Naga Agreement 2015,Bodoland peace accord etc

- **The Ministry of Development of North Eastern Region** Government of India ministry, established in September 2001, which functions as the nodal Department of the Central Government to deal with matters related to the socio-economic development of the eight States of Northeast India.

- **Development Aid**

Development aid for various infrastructure projects and improved connectivity trying to remove a sense of alienation among N-E people.

Way Forward

- India should not lower its guard regarding Naxalism and N-E insurgency. it should continue to be vigilant for emerging challenges
- The conflict in the NorthEast and LWE affected area is the physical manifestation of the aspiration of people. Thus there is a need to address the aspirations of the people by establishing continuous dialogues with them.
- As per ARC in extremist-affected districts, establishing and reinforcing local level police stations that are effectively staffed by local recruits should be a key component of the policing plan.
- Greater coordination between central forces and state forces for better tactical response.
- Roping in more NGOs and other groups that work with tribals in N-E region and LWE affected areas to help them get more skills and opening new vistas of employment based on their skills can help nip alienating feelings among them.

Role Of External State And Non-state Actors In Creating Challenges To Internal Security

First of all let us see the past year UPSC questions and understand their demand.

Questions	Keyword/Context/Demand
Indian Government has recently strengthened the anti-terrorism laws by amending the unlawful Activities (Prevention) Act (UAPA), 1967 and the NIA act. Analyze the changes in the context of prevailing security environment while discussing the scope and reasons for opposing the UAPA by human rights organizations. (2019, 15 Marks)	Prevailing security environment ,scope and reasons for opposing the UAPA by human rights organizations in context of prevailing changes
The banning of 'Jammatt-e-Islami' in Jammu and Kashmir brought into focus the role of over-ground workers (OGWs) in assisting terrorist organizations. Examine the role played by OGWs in assisting terrorist organizations in insurgency affected areas. Discuss measures to neutralize influence of OGWs. (2019, 10 Marks)	Role of over-ground workers (OGWs) in assisting terrorist organisation, measure for the same.
Analyse the multidimensional challenges posed by external state and non-state actors, to the internal security of India. Also discuss measures required to be taken to combat these threats. (2021, 15 Marks)	multidimensional challenges posed by external state and non-state actors, to the internal security of India.

Most of the points under this topic are covered in various chapters of our PRAYAAS Notes of Internal Security. Here we only look into detail about concepts of State actors and Non state actors.

External State actor

It is used in the context where one government supports an actor in the performance of an act or acts of terrorism against the other often deemed as a state sponsor

Challenges through Various External State actors

In context of India following 3 external state actors poses major challenge to internal security of India

- **Pakistan**

- Increasing activities of Pakistan's Inter-Services Intelligence (ISI) in Nepal changed the nature

of the border completely.

- It has ties with the Taliban and other radical groups.
- These groups have recently been involved with the radicalization of the Rohingya refugees in Bangladesh.
- Groups such as the Lashkar-e-Taiba (LeT), the Haqqani Network and the Taliban have repeatedly been used by Pakistan as instruments to help it achieve its foreign policy objectives in India and Afghanistan.
- **China**
 - The People's Liberation Army continues to deploy construction equipment for road works.
 - China's growing assertiveness in the region could be aimed at pushing Bhutan to agree to swap Doklam.
 - China is setting up villages in uninhabited tri-junction stretches between India, Bhutan and China, which are intended to support Chinese military facilities.
 - China is not following the resolution mechanism of maritime disputes in reference to the South China Sea where China is flexing its military muscle despite an international tribunal verdict (UNCLOS) going against it.
- **Bangladesh**
 - Huge Refugee influx.
 - Radicalisation of youth near border area

Non state actors

Organizations and individuals not connected with, directed by, or funded through the government are non-state actors. They can be corporations, NGOs, and even paramilitary and armed resistance groups.

Various non-state actors

- Terrorist organisations
- Drug cartels and gun runners
- Human-trafficking cartels
- Fake currency rackets
- Cyber attacks
- Maoists/Naxalites
- Insurgents/cross-border ethnic groups
- Illegal immigrants
- Trans-national/multinational corporations (TNC/MNC)

- Civil society organisations/NGOs
- Pirates
- Gamblers, foreign bookies and cricket mafias

All the non-state actors covered in various topic of Internal Security of PRAYAAS notes.



Challenges To Internal Security Through Communication Networks, Role Of Media And Social Networking Sites In Internal Security Challenges

First of all let us see the past year UPSC questions and understand their demand

Questions	Keyword/Context/Demand
What are social networking sites and what security implications do these sites present? (2013, 10 Marks)	Social Networking sites and their security implications
Religious indoctrination via digital media has resulted in Indian youth joining the ISIS. What is ISIS and its mission? How can ISIS be dangerous to the internal security of our country? (2015, 12.5 Marks)	Digital media and its role for youth radicalisation, ISIS
Use of internet and social media by non-state actors for subversive activities is a major security concern. How have these been misused in the recent past? Suggest effective guidelines to curb the above threat. (2016, 12.5 Marks)	Use of internet and social media by non state actors, Major security concerned associated with it.

Challenges to internal security through communication networks

Introduction

- Communication networks are a part of our critical information infrastructure which was **defined in the IT Act, 2000** as "the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety."
- Communication networks convey information from one point to the other. In this process, each communication link is subject to security threats and it has potential to pose a complex challenge to internal security.
- Communications networks are crucial to the connectivity of other critical infrastructure, viz. civil aviation, shipping, railways, power, nuclear, oil and gas, finance, banking, communication, information technology, law enforcement, intelligence agencies, space, defence, and government networks

Challenges to internal security through communication networks

Before going to challenges first we will look into various network threats

Following are common threat vectors attackers can use to penetrate any network.

- **Unauthorized access**

Unauthorized access refers to attackers accessing a network without receiving permission. Among the causes of unauthorized access attacks are weak passwords, lacking protection against social engineering, previously compromised accounts, and insider threats.

- **Distributed Denial of Service (DDoS) attacks**

Attackers build botnets, large fleets of compromised devices, and use them to direct false traffic at your network or servers. DDoS can occur at the network level, for example by sending huge volumes of SYN/ACC packets which can overwhelm a server, or at the application level, for example by performing complex SQL queries that bring a database to its knees.

- **Man in the middle attacks**

A man in the middle attack involves attackers intercepting traffic, either between your network and external sites or within your network. If communication protocols are not secured or attackers find a way to circumvent that security, they can steal data that is being transmitted, obtain user credentials and hijack their sessions.

- **Code attacks**

Many websites accept user inputs and fail to validate and sanitize those inputs. Attackers can then fill out a form or make an API call, passing malicious code instead of the expected data values. The code is executed on the server and allows attackers to compromise it.

- **Privilege escalation**

Once attackers penetrate your network, they can use privilege escalation to expand their reach. Horizontal privilege escalation involves attackers gaining access to additional, adjacent systems, and vertical escalation means attackers gain a higher level of privileges for the same systems.

- **Insider threats**

A network is especially vulnerable to malicious insiders, who already have privileged access to organizational systems. Insider threats can be difficult to detect and protect against, because insiders do not need to penetrate the network in order to do harm. New technologies like User and Even Behavioral Analytics (UEBA) can help identify suspicious or anomalous behavior by internal users, which can help identify insider attacks.

- **Threat regarding Hardware and ownership**

- Much of the hardware and software that make up the communications ecosystem is sourced externally. Foreign governments are taking advantage of the market penetration and dominance of their companies to infiltrate and compromise telecommunications networks.
- The task of securing the networks is also complicated by the fact that much of the infrastructure is in the hands of private companies. These private firms frequently compromise network security. Recently Chinese company Huawei faced backlash for the same in USA.

All these network threat cumulatively create various Internal Security challenges these challenges are as follows

- Economic threats such as frauds, attack on banking communication infrastructure, acquisition of critical data such as customer's credit/debit card data, Financial theft to destabilize the economy. All these economic threats cumulatively used in cyberwarfare which is one of the major threat to internal security.
- Information warfare to run propaganda by anational element.
- Destabilizing critical infrastructure like Nuclear power plants, power grids, Dams, Share Market operations through cyber attacks.
- Penetrating value chain of production of communications network infrastructure for spying purpose.
- Target to public portals through communication networks and disrupting the daily public system.
- Leakage of sensitive information like defence and Security through attack on communication networks.

Steps taken by Government

- National Security Directive on Telecommunication Sector 2021. Under the provisions of this directive, the government will declare a list of trusted sources and trusted products for installation in the country's telecom network.
- Indigenisation technology. Recent 5G launch in India through indigenously developed technology.
- Promotion for manufacturing critical infrastructure hardware components in India under National electronic policy.
- Information Technology Act 2008: under this act various network threats are taken into account.
- Telecom Regulatory Authority of India (TRAI): It regulates licensing of communication network in India.
- National Digital Communications Policy in 2018: DoT may have legitimate grounds for extending its jurisdiction over digital communications and various digital applications.

You can also use **steps taken** which are explained under the cybersecurity topic in Prayas Internal Security notes.

Role of media and social networking sites in internal security challenges

Introduction

For a nation like India, access to information and freedom of expression continue to be the foundation of its democracy and the champion of its national interests. In this media plays a vital role. The digital revolution has exponentially increased the reach of traditional/digital media and social media. But the same media act as a double-edged sword in the internal security regime. The potential of threats emanating from media to internal security are immense. Here we are going to discuss both traditional media and Social media separately.

1. Challenges associated with media to internal Security

- Sensationalization of news without verifying proof of the news by news channels may create law and order problems.
- Petty TRP race of media creates problems like insensitive treatment of national security issues. The media reporting of 26/11 was criticized for divulging critical information.
- Polarising news reporting may fuel communal tensions which is always harmful to internal security.
- The post-truth media bases its arguments on emotions and not solely on facts making it vulnerable to breach by enemy and manipulations.
- Media's reporting on terrorism has been questioned from time to time. It scapegoats one community, promotes warmongering, and shapes public opinion for the drastic and sudden measures to tackle terrorism which are not always wise.
- The electronic media's focus on profit-making is making it invest more on peripheral matters rather than the core job of news reporting this tendency may promote fake news culture which is always harmful to Internal Security.

2. Challenges associated with Social Networking site to Internal Security

- Could be used as a weapon for influencing public sentiment by external state and non state actors.
- Social media platforms like Facebook pages and WhatsApp groups could be used as propaganda machines. They act as echo chambers of radicalism and result in radicalized citizenry.
- Social media is increasingly being used to propagate religious fundamentalism this could be harmful to communal harmony.
- Tool by terrorist organisation for recruitment of terrorist.
- Rising troll culture and online abuse, death/rape threats on social media may create law and order problems.
- Social media is beyond traditional regulation and its transnational nature may create news security challenges.

Steps Needed to contain the security issue through media and Social Networking sites

- Public awareness is key to regulating both traditional media and Social media.
- The PCI (Press Council of India) can be given penalizing power so that it can better manage the media for professionalism and information accuracy.
- News Broadcasting Standards Association should take measures to contain sensationalism and TRP hunger in News channels.
- Institutionalizing the blueprint of national social media policy to monitor and regulate social media for security threats.

- Taking social media giants on board to tackle the use of social media for criminal and anti-national activities.
- Smart policing must be the new face of policing in India. Digital training of police must be done to better equip them against online threats and instances of cyberterrorism.
- Social media analysis generated intelligence or SOCMINT is being developed as a successful model in many countries abroad to isolate hotspots or subjects that go viral and is used as a predictive tool. India can use this for controlling menace of fake news.



Basics of cyber security

First of all let us see the past year UPSC questions and understand their demand.

Questions	Demand/Context/Keywords
Cyber warfare is considered by some defense analysts to be a larger threat than even Al Qaeda or terrorism. What do you understand about 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. (2013, 10 Marks)	Cyber Warfare, cyber threat posed by india, preparedness.
Considering the threats cyberspace poses for the country, India needs a "Digital Armed Forces" to prevent crimes. Critically evaluate the National Cyber Security Policy, 2013 outlining the challenges perceived in its effective implementation. (2015, 12.5 Marks)	Cyberspace, National Cyber Security Policy, 2013
Discuss the potential threats of Cyber attack and the security framework to prevent it. (2017, 10 marks)	Potential threat of cyber attack, Security framework for the same.
Data security has assumed significant importance in the digitized world due to rising cybercrimes. 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 protection of personal data in cyber space? (2018, 15 Marks)	Data security, B.N Srikrishna committee Report.
What is the CyberDome Project? Explain how it can be useful in controlling internet crimes in India. (2019, 10 Marks)	Cyberdome Project
Discuss different types of cybercrimes and measures required to be taken to fight the menace. (2020, 10 Marks)	Different types of cybercrime, Measure to control these crime.
Keeping in view India's internal security, analyse the importance of cross-border cyber attacks. Also discuss defensive measures against these sophisticated attacks. (2021, 10 Marks)	Cross border cyber attack, defensive measure

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. (15 marks)	Element of cyber security, Comprehensive national cybersecurity Strategy
---	--

What is cyber security?

Definition - Cyber security is the practice of protecting cyberspace(critical systems,Networks, Programmes and sensitive information) from digital attacks.

DIFFERENT ELEMENTS OF CYBER SECURITY

- **Application security**

Practice of adding security features within applications during development period to prevent from cyber attacks

- **Information security**

It is the process and methodology for preventing unauthorized access, use, disclosure, disruption, modification, or destruction of information.

- **Disaster Recovery Planning**

It includes strategies and preparations in case of cyber attack like data protection measure, data recovery plan, cloud backup etc

- **Network Security**

Process of preventing and protecting networks and devices connected it from suspicious network behavior.

- **End-user Security**

It consists of cyber security awareness for end users of cyberspace.It is the most important element, more than 90% of cyber attacks begin with a phishing e-mail.

- **Operational Security**

It is procedural security.It identifies the organization's critical information and develops a protection mechanism to ensure the security of sensitive information.

Various cyber threats -

Based on motive and perpetrators cyber threats categorised in

1. Those directed to computer or other devices and networks

- **Cyber espionage**

Cyber espionage also called as cyber spying is the strategy of breaking into a computer system and network.In which an unauthorized user attempts to access sensitive or classified data or intellectual property (IP) for economic gain, competitive advantage or political reasons.

Eg. Attack on Kudankulam Nuclear power plant 2019-suspected cyber espionage by china

- **Malware**

Malware (short for "malicious software") is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants

Eg. CovidLock, ransomware, 2020-targeting system through malicious files claiming to offer information about the disease.

After installation, the ransomware encrypts all data on Android devices and denies the user access. To recover your files, you're required to pay a ransom of \$100 per device.

- **Ransomware**

Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key.

Eg-Wannacry,Petya.

- **Phishing**

Phishing is a cybercrime in which malicious actors send messages pretending to be a trusted person or entity.

Eg.Fake messages of HR,fake Credit card e-mail.

- **SQL Injection attack**

SQL Injection is a web vulnerability caused by mistakes made by programmers. It allows an attacker to send commands to the database that the website or web application communicates with.

Eg-Cisco vulnerability—in 2018, a SQL injection vulnerability was found in Cisco Prime License Manager. The vulnerability allowed attackers to gain shell access to systems on which the license manager was deployed

- **Botnet**

It is a set of compromised computers which are under control of the attacker.

Eg.The 2016 Mirai Attack- Mirai was a botnet consisting of more than 100,000 computers. It launched attacks against several cybersecurity companies and affected their critical infrastructure.

2. Cyber terrorism -

- Cyberterrorism refers to any premeditated, politically motivated attack against information systems, programs and data that threatens violence or results in violence.
- It uses all cybercrime tools like cyber espionage,malware,ransomware..etc Eg-as per Center for Strategic and International Studies (CSIS), a bipartisan, nonprofit policy research group, in 2021 A Russian group claimed responsibility for a ransomware attack on CS Energy, an Australian utility company,was one of the cyber terrorism incident.

3. Cyber Warfare

Cyber Warfare is defined as a set of actions by a nation or organization to attack countries or institutions computer network systems with the intention of disrupting, damaging, or destroying

infrastructure by computer viruses or denial-of-service attacks.

Eg-Operation Shady RAT is an ongoing series of cyber attacks starting mid-2006, reported by Internet security company McAfee in August 2011. China is widely believed to be the state actor behind these attacks which hit at least 72 organizations including governments and defense contractors.

4. Using cyberspace for Social engineering and personal attacks

- Cyber bullying and stalking
- Child pornography
- Honeytrap
- Using social media for propaganda, recruitment, radicalisation by terrorist organisation

Issues associated with cybersecurity

Parameter	Issue	Impact
1. For individual	<ul style="list-style-type: none"> • Lack of Awareness • Digital device 	<ul style="list-style-type: none"> • Inappropriate use of information by individual • Compromise with individual data. <p>Eg. leaks of Covid-19 test results due to lack of awareness</p>
2. For corporates	<ul style="list-style-type: none"> • Lack of skilled labour for handling cybersecurity issues • Corporate battles 	<ul style="list-style-type: none"> • Affects corporate profit which directly impact overall economy of countries • Cybersecurity threats creates hesitancy regarding adaptation of new technology
3. For Nation (specifically India)	<ul style="list-style-type: none"> • Absence of robust cybersecurity policy • Lack of coordination. <p>Eg-collusion of state and centre laws/policies in india regarding cyberspace</p> <ul style="list-style-type: none"> • Foreign dependency <p>Eg-Chip import</p> <ul style="list-style-type: none"> • Absence of data protection policy 	<ul style="list-style-type: none"> • Large scale critical infrastructure with poor cybersecurity and privacy features make them prone to cyberattack <p>Eg-Power grid, defence infrastructure, banking..etc.</p> <ul style="list-style-type: none"> • May affect government initiative like Digital india, various e-governance tools this will directly impact on inclusive growth. • Threat of anti-national activit like radicalisation, recruitment through social

		media platforms by terrorist organisation. • Internal and external security risk from both state and non state actors from cyber attack.
4. Other Parameters	<ul style="list-style-type: none"> • Emerging Technologies Eg-Block chain, Web3, Internet of Things. etc • Emergence of cyberspace fifth arena of war (Land, water, air, space) 	<ul style="list-style-type: none"> • Organised crime at global level Eg-cryptocurrency use for money-laundering, drug trafficking. • Cyber warfare Eg-In 2007 a three week wave of massive cyber attack against Estonia from part of private Russian citizens

Cyber Security scenario in India

- India ranks 3rd in terms of the highest number of internet users in the world after USA and China.
- India was ranked among the top five countries to be affected by cybercrime, according to a 22 October report by online security firm "Symantec Corp".
- As per the data by NCRB (National Crime Record Bureau), 12317 cases related to cybercrime were registered in 2016.
- India ranked 10th out of 165 nations in the second Global Cybersecurity Index (GCI)

Steps taken

- **Information technology (Amendment) Act 2008**-It has been enacted to cater the needs of National cyber security by addressing host issues like technology related cyber crimes, data security and privacy protection.
- **National Critical Information Infrastructure Protection Centre (NCIIPC)** established for protection of critical information infrastructure in the country.
- **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)**-Launched for providing detection of malicious programmes and free tools to remove such programmes.
- **The Indian Computer Emergency Response Team (CERT-In)**

It is an Emergency Response Team which operates as the national agency to address the country's cyber security, which helps in reducing the rate of cyber attacks on government network.

- **Cyber Surakshit Bharat**

It is Initiative of the Ministry of electronics & IT. Which aims to strengthen the cybersecurity ecosystem in India for the Government's vision of a "digital India".

- **Indian cyber-crime coordination centre(I4C)**

Indian Cyber Crime Coordination Centre (I4C)" is an initiative of the Ministry of Home Affairs

(MHA) to combat cyber crime in the country, in a coordinated and effective manner.

- **National cybersecurity coordination centre**

It is under the National Security Council Secretariat (NSCS). coordinates with different agencies at the national level for cyber security matters.

Lacunae in current cybersecurity measures

1. Absence of proper legislative framework for data protection.
2. Lack of Coordination among various stakeholders Eg-Between centre state, between private player and government..etc
3. Inadequate coverage of many emerging cyber issues like Copyright infringement, cryptocurrency, spam emails. etc
4. Extremely low Conviction rate for cyber crimes.
5. Absence of a comprehensive and well-defined information sharing model among various stakeholders in cyberspace.
6. Lack of standard procedures for seizure and analysis of digital evidence.

Way forward

1. **Policy oriented solution**

- Comprehensive legal framework for data protection.
- Integrated cybersecurity command for coordination in tackling cyberattacks.
- Dedicated cadre of officers for cyberspace.

2. **Technological solutions**

- Artificial intelligence and machine learning can boost cyber defence
- Blockchain and Non Fungible Token(NFT) technology for reducing cyber theft.
- Promoting indigenisation of critical infrastructure hardware components.
- Harnessing advantage of quantum technology for secure data transfer

3. **Human resource :**

Immediate attention to human resource development for reducing skill gaps in cyber security.

4. **Implementing Gulshan Rai committee recommendations.**

- Reducing dependency on foreign servers by creating one dedicated secure gateway for all government communication.
- Establishing a new Indian Cyber Crime Coordination Centre which could be linked to NATGRID and CCTNS (Crime and Criminal Tracking Network system)
- Establish a separate agency for online cybercrime.

Best practices

- **Israel National Cyber Bureau** Created in 2012, it is instrumental in creating a national cyber

defence policy, partnerships with the private sector, and linking domestic and international cyber defence players.

- **Cyberdome kerala**

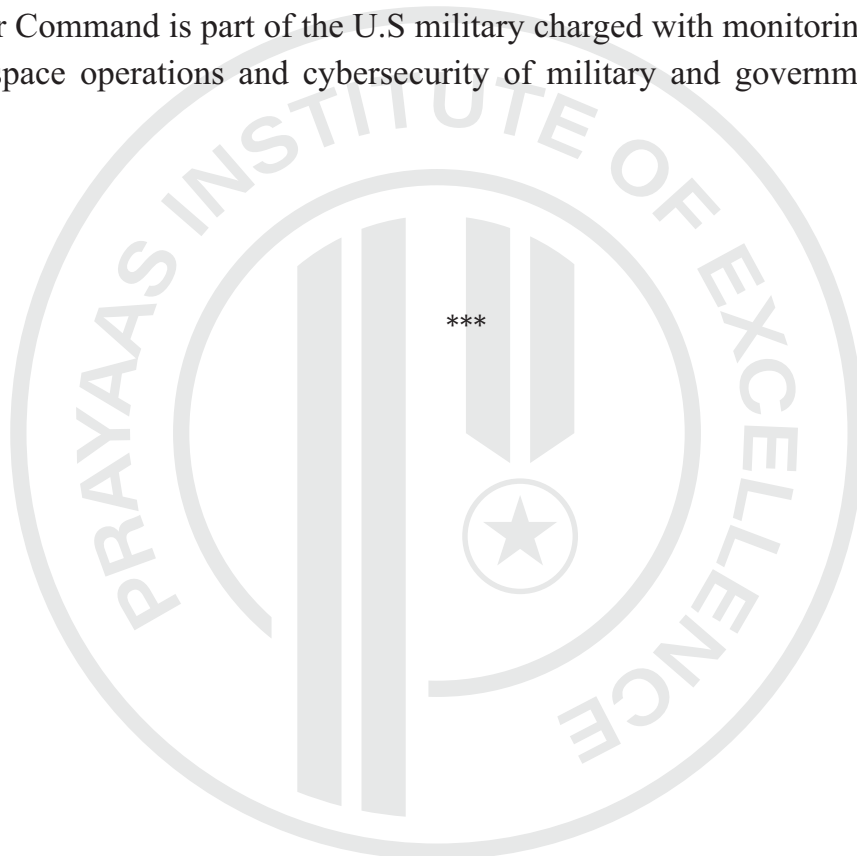
It is research and development centre of Kerala Police Department, acts as a cyber centre of excellence in cybersecurity, as well as technology augmentation for effective policing.

- **Estonia**

In 2007, a three week wave of massive cyber attacks temporary shutdown of government functions, also economic activities. This was world's first cyber war which gave Estonia an experience necessary to rise to the top of the cybersecurity world in both the private and the public sector. Today Estonia among top three in global cyber security index.

- **UNITED STATES CYBER COMMAND**

The U.S. Cyber Command is part of the U.S military charged with monitoring and managing the existing cyberspace operations and cybersecurity of military and government IT and Internet operations.



Money-Laundering And Its Prevention

First of all let us see the past year UPSC questions and understand their demand.

Questions	Keyword/Context/Demand
1. 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? (2013, 10 Marks)	Key Security challenges with Money Laundering
2. Discuss how emerging technologies and globalization contribute to money laundering. Elaborate measures to tackle the problem of money laundering both at national and international levels. (2021, 10 Marks)	Emerging Technologies and Money Laundering. National and international framework for tackling money laundering.

Very few questions asked on this but till it is one the most discussed topic in news so don't ignore this. Questions are very straight forward considering current context from new tackle these questions. So first understand thoroughly about this topic.

What is Money Laundering?

General Definition: Money laundering is the process of hiding the source of money obtained from illegal sources and converting it to a clean source, for the purpose of avoiding prosecution, conviction, and confiscation of the criminal funds.

As per UN Vienna 1988 Convention : Money Laundering is, "the conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions".

As per FATF : The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source.

Stages of Money Laundering

- 1. Placement :** Introducing the funds in banking and financial system
- 2. Layering :** By series of financial operation giving these funds appearance of having legal origin.
- 3. Integration :** Once these funds get legal appearance reintroducing these funds in the legal economy. ex:consumption of luxury goods, share market and real estate investment.

We can also understand money laundering from following figure :

HOW DIRTY MONEY IS LAUNDERED

Typical Money Laundering Scenario



Purpose of Money laundering

- Tax evasion.
- Theft.
- Fraud.
- Bribery.
- Corruption.
- Smuggling.
- Modern slavery.
- Human trafficking.
- Drug trafficking.
- Illegal arms sales.

Various Methods of Money laundering

- **Smurfing** : Involving structuring of large amounts of cash into multiple small transactions.
- **Shell companies** : Entity that does not have active business operations but is set up to achieve specific business objectives such as reducing tax liabilities, shielding an entity from legal risks, raising capital, and oftentimes, for illegal purposes such as laundering money, hiding beneficial ownership from law enforcement or circumventing sanctions.
- **Round tripping** : Unethical practice of purchasing and selling shares of the same security over and over again in an attempt to manipulate observers into believing that the security is in higher demand than it actual.
- **Trade based money Laundering** : use of trade transactions in an attempt to legitimise illicit origins of money.
- **Hawala** : Hawala is an informal money transfer system in which money is passed on through a

network of brokers (known as hawaladars) without cash's actual/physical movement.

- **Gambling** : In this proceeds from casinos, betting taken into account to transform illicit money into legitimise money.
- **Agriculture Income** : Though agricultural income in india non taxation. Using this lacuna for converting illegal money into legitimise source.
- **Cash intensive Businesses** : Using cash intensive business account for money Laundering.
- **Digital form of Money laundering**
development of technology in the financial sector creating new money laundering threats. These threats pose from cryptocurrency, E-commerce, online gambling and video games.

Impact of Money Laundering:

1. Economic impact

- Affect money demand in the economy which may distort and instability in the economy.
- Inflation in the economy.
- Discourage foreign investment.
- Directly affect the welfare of the general public.
- Threat of loss of control of economic policy.
- Reduction in tax revenue.

2. Social Impact

- Human trafficking.
- Socio-cultural disintegration.
- Increased criminality in society.
- Drug addiction.
- Affect societal morality

3. Political impact

- Criminalisation of politics
- Political instability.
- Corruption.
- Dent on political image of the country at global level. like FATF grey & black list.

4. Security impact

- Terror financing.
- Arms trafficking.
- Creating instability in the country through proceeds from money Laundering like Militancy, Naxal

activity.. etc.

- Organised crimes like drug trafficking.

Current framework for Money laundering

In india

1. Legal framework

These are old laws but use them in your answers just put reference of these laws

- The Income Tax Act, 1961.
- The Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974
- The Benami Transactions (Prohibition) Act, 1988
- The Foreign Exchange Management Act, 2000 (FEMA)

Now we can see some of the recent legal framework. There might be chances of being asked in exam. Otherwise use these laws in your answers effectively.

- **Prevention of Money laundering act 2002**

few core objectives of PMLA

- Prevention and controlling money laundering.
 - Confiscation and seizing of property involved in or derived from money laundering.
 - Providing punishment to offenders
 - Appointment of adjudicating authority and appellate tribunal concerning money laundering matters
 - Maintaining records and putting obligations on financial institutions, banking companies and institutions
 - Dealing with every issue related to money laundering.
- **NIA act 2008**
- NIA (Amendment) Bill, 2019 to the NIA Act has brought the offences related to the smuggling in High-Quality Counterfeit Indian Currency under the definition of a terrorist Act. Which is directly related to Anti Money laundering step.

- **Fugitive Economic offender act 2018**

The Fugitive Economic Offenders Act, 2018 empowers any special court (set up under the Prevention of Money Laundering Act, 2002) to confiscate all properties and assets of economic offenders who are charged in offences measuring over INR 100 crores and are evading prosecution by remaining outside the jurisdiction of India.

2. Institutional Measure

- **Enforcement Directorate**

It is established in the year 1956. which is responsible for enforcement of the Foreign Exchange

Management Act, 1999 (FEMA) and certain provisions under the Prevention of Money Laundering Act.

- **NIA**

Looks into issue of terror financing and money laundering under NIA act. Terror funding and Fake currency cell also works under NIA

- **Combating Financing of Terrorism (CFT) cell**

Established under Ministry of Home affairs. It coordinates with different investigation agencies for cases pertaining to money laundering.

- **Financial Intelligence Unit-India**

Established by the Government of India in 2004 as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect financial transactions. It is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

International Cooperation

- **Vienna Convention, 1988**

It recognized that money laundering was the powertrain of criminal enterprises engaged in drug trafficking, especially because they used global banking operations to exploit breaches in international laws and enforcement to mobilize their financial resources.

- **The 1990 council of Europe convention**

The Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, drawn up within the Council of Europe by a committee of governmental experts under the authority of the European Committee on Crime Problems (CDPC).

- **SDG**

SDG target 16.4 talks To reduce illicit financial flows, strengthen recovery and return of stolen assets, and combat all forms of organized crime

- **FATF :**

It is an intergovernmental body established by the G7 summit in Paris in 1989 .It is responsible for setting global standards on anti-money laundering and combating financing of terrorism.

- **Egmont Group:**

Facilitates and prompts the exchange of information, knowledge, and cooperation amongst member FIUs to combat money laundering, terrorist financing, and associated predicate crimes.

Use these institutional structures and global conventions in your answers. This will provide authenticity to your answer.

Challenges in preventing Money Laundering

- **Complicated procedures**

Complicated procedure in law itself creates hindrance in Anti Money Laundering drive.

- **Multiple Lawas and Multiple agencies**

In India itself for handling money handling cases there are multiple Laws and agencies as we discussed above. This multiplicity further complicates the process.

- **Tax haven countries**

Investment in tax havens (such as Hong Kong, the Cayman Islands, and the British Virgin Islands) is a major component of money laundering.

- **Widespread act of smuggling**

Black Market channel and criminal nexus further created hindrance in tackling money laundering

- **Emerging Technologies**

Emerging technologies like Cryptocurrency, IoT & Web3 creating new challenges for Anti Money Laundering drive.

Generic points

- **Lack of skilled personnel.**
- **Lack of coordination among various agencies**
- **Political interference in cases**
- **Lack of awareness.**

Way forward

- **Rationalisation of tax rates**

To prevent tax evasion

- **Improve Searches with Technology**

Using technology, such as AI, to conduct constant searches can help to reduce some of the burden for Anti Money Laundering officials. Also Use of Data Analytics to Find Patterns of money laundering

- **Regular Cross-Communication.**

Cross communication between banks, law enforcement agencies and other financial institutions.

- **Global partnership** both at Bilateral level and multilateral level.

- **Structured Training**

Training for handling critical cases.

- **Implementing FATF Recommendations** for Money Laundering at National and international levels.

Security Challenges And Their Management In Border Areas

First of all let us see the past year UPSC questions and understand their demand.

Questions	Keyword/Context/Demand
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? (2013, 10 Marks)	Border management and internal security
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. (2014, 12.5 Marks)	Transborder migration and security challenges
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. (2016, 12.5 Marks)	Challenges associated with effective Border management.
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 Marks)	Transborder insurgency and security challenges in North East India
Analyse internal security threats and transborder crimes along Myanmar, Bangladesh and Pakistan borders including Line of Control(LoC). Also discuss the role played by various security forces in this regard. (2020, 15 Marks)	Transborder crimes and role of Security forces tackling these crimes
For effective border area management, discuss the steps required to be taken to deny local support to militants and also suggest ways to manage favourable perception among locals. (2020, 10 Marks)	Local support for effective Border management

<p>What are the maritime security challenges in India ? Discuss the organisational, technical and procedural initiatives taken to improve maritime security. (2022, 10 marks)</p>	<p>Maritime security challenges</p>
---	-------------------------------------

Introduction

According to the UNSC border management is the first line of defence against the movement of terrorists across borders and the illegal cross-border movement of goods and cargo.

Border management is an integral part of India's defence and commerce. India's border management comprises border security, border region development, communication, and coordination with the neighbouring states and programs to enhance the national interests of India.

There are two aspects of border in international scenario:

1. Land Border
2. Maritime Border

1. Land Border Management

India shares border with following states

- Bangladesh (4,096 km).
- China (3,488 km).
- Pakistan (3,323 km).
- Nepal (1,751 Km).
- Myanmar (1,643 Km).
- Bhutan (699 Km)
- Afghanistan (106 Km)

In Indian case complexity and extreme geography (Desert, mountain terrain,swamp region and forest area) offers different challenges for Effective Border Management.

So here we can study different challenges along different borders of India in tabular form.

Border	Challenges	Steps taken by government
Pakistan	<ul style="list-style-type: none"> • Disputed area like Sir Creek and Loc • Terrorist intrusion from other side of border • Insurgency in Kashmir along Loc • Proximity to the Golden crescent adds threat of drug trafficking. • Fake currency and arms trafficking • Movement of drones for airdropping drugs, arms and ammunition from Pakistan. 	<ul style="list-style-type: none"> • Comprehensive Management System (CIBMS) to establish an integrated security system at borders providing all round electronic surveillance even in adverse climatic conditions. • Project BOLD-QIT (Border Electronically Dominated QRT Interception Technique) under Comprehensive Integrated Border Management System (CIBMS) • Mission AABAD' 30 for border village development. • Reservation benefits to people living along Indo-Pak border in Jammu and Kashmir
China	<ul style="list-style-type: none"> • Undemarcated border due to complex topography of region. • High border area infrastructure investment from China. • Claim of China over Arunachal Pradesh. • Aggression of China in Ladakh area • Smuggling of electronic and other cheap Chinese goods. 	<ul style="list-style-type: none"> • Push for new infrastructure development along the Indo China border. eg. Dhola Sadiya bridge. • Forest clearance for Army infrastructure project along LAC within 100 km range. • Vibrant Villages Programme for Northern border of country for more robust border area development • Deployment Special Frontier Force (SFF) or Vikas regiment in Ladakh
Bangladesh	<ul style="list-style-type: none"> • Porous nature of border • Difficulty in identifying Bangladeshi nationals. • Change of Profile of Border Areas- Continuous influx of illegal migrants has resulted in a change of profile of the border areas. • Human Trafficking. • Smuggling of Cattles, drugs, arms, fake currency and gold. 	<ul style="list-style-type: none"> • Comprehensive Border Management Plan (CBMP) to control border crimes. • Subregional connectivity project. eg. Agartala-Akhaura Rail-Link • India Bangladesh Land Boundary Agreement, 2015 • Raising awareness by BSF and BGB (border guard Bangladesh) among the locals regarding crime prevention in the border area.

<p>Myanmar</p>	<ul style="list-style-type: none"> • Porous nature of border • Difficulty in identifying Bangladeshi nationals. • Change of Profile of Border Areas- Continuous influx of illegal migrants has resulted in a change of profile of the border areas. • Human Trafficking. • Smuggling of Cattles, drugs, arms, fake currency and gold. 	<ul style="list-style-type: none"> • Free movement regime(FMR)- misuse of FMR for insurgency in North East. • Proximity to the Golden triangle creates the challenge of drug trafficking. • Porous border with weak infrastructure along the border area. • Hardship in border patrolling due to difficult terrain and dense forests. • Illegal migration due to Rohingya crisis
<p>Myanmar</p>	<ul style="list-style-type: none"> • Free movement regime(FMR)- misuse of FMR for insurgency in North East. • Proximity to the Golden triangle creates the challenge of drug trafficking. • Porous border with weak infrastructure along the border area. • Hardship in border patrolling due to difficult terrain and dense forests. • Illegal migration due to Rohingya crisis 	<ul style="list-style-type: none"> • Kaladan Multi-Modal Transit Transport Project for connectivity. • Mekong-Ganga Cooperation. • Act East initiative.
<p>Nepal</p>	<ul style="list-style-type: none"> • Misuse of open border by local criminal gangs and external state actors(China,Pakistan)for destabilising india. • Smuggling of arm and ammunition. • Illegal immigration for economic reasons, • Territory dispute like Kalapani, Susta. 	<ul style="list-style-type: none"> • Development aid to Nepal. • Act East policy. • Nepal Bharat Maitri Emergency and Trauma Centre in Kathmandu. • Establishment of a new intelligence section in SSB (Sashastra Seema Bal)at Indo-Nepal and Indo- Bhutan border to for better operational efficiency
<p>Bhutan</p>	<ul style="list-style-type: none"> • Tri-junction dispute. • Use of Bhutan territory by insurgent groups for anti India activity. • Porous Border leads to Smuggling of goods such as Bhutanese cannabis, liquor and forest products. 	<ul style="list-style-type: none"> • Act East policy • Strong bilateral relations. • Power purchasing agreement

In exam hall if you fail to recollect specific challenges then use following generic points which applies for each border area

- Illegal migration especially along Bangladesh and Nepal borders
- Counterfeit Currency issues
- Human trafficking
- Terrorism, mainly from Pakistan
- Smuggling of arms and ammunition
- Drug smuggling
- Support to Left-wing extremism
- Armed succession struggle

2. Coastal Border Management

India has a coastline of 7,517 km, of which the mainland accounts for 5,422 km. Post-Mumbai attacks in 2008, the lacuna of Indian coastal security reflected in front of world.

Challenges of coastal security in India

- Maritime Terrorism: It is quite possible for rival interests to take advantage of this extensive maritime activity to launch attacks on land, as was seen in the Mumbai terror attacks of 26/11.
- Disputed Maritime Boundary-India's maritime boundaries with Pakistan and Bangladesh are not delineated because of overlapping claims.
- Smuggling and trafficking: proximity to Pakistan, Bangladesh and Gulf coast creates challenges like smuggling of items such as gold, electronic goods, narcotics, and arms.
- Infiltration, illegal migration-refugee influx from Bangladesh, Myanmar (Rohingya refugee)
- Fragmented approach for coastal security-Multiplicity authorities like Navy, coast guards, state police just hampers comprehensive decision making.
- Challenge from external state actors-threat from Chinese naval activity in Indian Ocean region. Extra Regional Military Presence of Chinese Navy and its acquisition of a base in Djibouti, 24 access facilities in Malaysia, the "covert" base in Gwadar, and the recently announced maritime silk route are very concerning for India.
- Illegal unreported and unregulated fishing-paves way for piracy, trafficking and smuggling.

Maritime security initiative by Government

Currently Maritime security comes under domain of coast guard, Indian Navy and respective State police along with this govt took following steps.

- **Coastal Security Scheme (CSS)**

The CSS is a scheme steered by MHA for strengthening coastal policing wherein the MHA provides financial assistance to the states and Union Territories for infrastructure development, and procurement of vehicles and boats.

- **SAGAR or 'Security and Growth for all in the Region'**

To focus on cooperative measures for sustainable use of the oceans. The mission also provides a framework for a safe, secure, and stable maritime domain in the region.

- **Electronic Surveillance:** National Command Control Communication and Intelligence Network (NC3I) has been launched to provide near gapless surveillance of the entire coastline and prevent the intrusion of undetected vessels, the coastal surveillance network project. It comprises: Coastal radar chain, Automatic identification system (AIS), Vessel traffic management and information system (VTMS).

- **SAGARMALA**

For port led infrastructure development along the coastal area.

- **centralized database of fisherman and fishing vessels**

Issue of ID cards to all fishermen with a single centralised database, registration of over 2 lakh fishing vessels operating off our coast and equipping fishing boats with suitable equipment, to facilitate vessel identification and tracking are some of the other steps taken

- **Engagement**

Engagement for comprehensive Maritime security through initiative like QUAD, Malabar exercise, Indian Ocean Naval Symposium. etc

Way forward

- India needs a single agency to guard its borders-This will help in comprehensive decision making.
- Creating the sufficient physical infrastructure for movement of forces and logistics.
- Need to harness the advantage of technology for both land and coastal border management.
- Capacity building of defence agencies, central security forces and state police along the border line for better border Management.
- As per the Shetkar **Committee** there is a need to speed up road construction, various other infrastructure development projects which will lead to socio economic development in border areas.
- As per **G.P Bhatnagar committee** There should be lateral induction from the army to the para-military forces so as to enhance their operational effectiveness. This will be directly beneficial for effective border management.
- Engagement with neighbouring countries both at Bilateral and Multilateral forums for peaceful borders.

Linkages Of Organized Crime With Terrorism

First of all let us see the past year UPSC questions and understand their demand.

Questions	Keyword/Context/Demand
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? (2014, 12.5 Marks)	Piracy, Maritime security concerns
"Terrorism is emerging as a competitive industry over the last few decades." Analyse the above statement. (2016, 12.5 Marks)	Terrorism as competitive industry
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? (2017, 15 Marks)	Terrorism as challenge to National security, Sources of terrorist funding.
India's proximity to the 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 counter measures should be taken to prevent the same? (2018, 15 Marks)	linkages between drug trafficking and other illicit activities and Measure for the same
Analyse the complexity and intensity of terrorism, its causes, linkages and obnoxious nexus. Also suggest measures required to be taken to eradicate menace of terrorism. (2021, 15 Marks)	complexity and intensity of terrorism, It's linkages with other organised crime.
Discuss the types of organised crimes. Describe the linkages between terrorists and organised crime that exist at the national and transnational levels. (2022, 10 marks)	Types of organised crimes, linkages between terrorists and organised crime

This topic covers most of the other internal security topic which directly or indirectly links with organised crime and terrorism.

Organised crime

Introduction

A criminal wrong is more graver than a civil wrong as it is considered as an act against the whole society. Increasing crimes in any legal system are an example of a chaotic and alarming situation for the country. In this certain crimes are performed repeatedly by certain criminals, to not take revenge but to gain profits. Such instances fall under the scope of organised crimes. The same organised crimes always affect a nation's Economy, polity and Security.

Concept of organized crime

General definition - Organized crime means the commission of a crime at regular intervals in order to make money or profits.

As per "Maharashtra control of organized crime act, 1999." Organized crime" means any continuing unlawful activity by an individual, singly or jointly, either as a member of an organised crime syndicate or on behalf of such syndicate by using violence or threat of violence or intimidation or coercion, or other unlawful means, with the objective of gaining pecuniary benefits, or gaining undue economic or other advantage for himself or any person or promoting insurgency.

In the United States, the Organized Crime Control Act (1970) defines Organized crime as "the unlawful activities of a highly organized, disciplined association"

Nature of organized crime

- **Commission of crime**

To commit a crime (including organised crime), there are four stages that need to be fulfilled. First, there should be an intention to commit a crime. Secondly, there must be some preparation to give effect to the crime. Third, there should be an attempt, i.e., presence of some action in pursuance of the crime being committed. Lastly, the attempt should be accomplished for the commission of that crime.

- **Objective of earning profits**

The purpose of committing an organised crime is not to take revenge or harm someone, rather it is a kind of illegal business or a way for people to earn profits.

- **Regularity**

It is not a one-time event, but rather on a regular basis, just as a business.

Types of organized crimes

- **Money laundering**

- **Cybercrime**

- **Smuggling.**

To import or export something in violation of the customs laws. It is highly prevalent criminal activity in developing countries like India. Among the items smuggled into the country, gold tops the list in terms of supply and demand.

Trafficking in drugs is perhaps the most sinister of all the smuggling activities.

- **Drug Trafficking**

It is usually considered that the most important reason for the high rate of drug trafficking is the

geographical condition of India. It is located between the Golden Triangle (Myanmar, Thailand, and Laos) on the northeast and Golden Crescent (Pakistan, Afghanistan, and Iran) on the northwest-both of which are the two largest sources of illicit drugs in Asia.

- **Organized gang criminality:**

Bank robbery, hijacking, murder, kidnapping, automobile and jewel thefts are some of the common examples.

- **Human trafficking**

Human trafficking is a global crime that trades in people and exploits them for profit. People of all genders, ages and backgrounds can become victims of this crime, which occurs in every region of the world. Traffickers use violence, fraudulent employment agencies, and fake promises of education and job opportunities to trick, coerce and deceive their victims

- **Racketeering:**

Extorting money from legitimate or illegitimate business amounts to what is known as Racketeering. Most of the time illegal business are more prone to racketeering

- **Counterfeiting :**

A counterfeit is an item that uses someone else's trademark without their permission. By making or selling a counterfeit, criminals seek to profit unfairly from the trademark owner's reputation.

- **Syndicate Crime**

This is the most significant area of organized crime and consist of the supply of illegal goods and services; smuggling, bootlegging, gambling, prostitution and foreign exchange violations are examples of such crimes.

Challenges in controlling the organised crime

- **Law-making and enforcement**

Currently there is no central legislation specifically governing organised crime in India.

- **Slow trials**

These organised criminals are tried under different laws, the whole process of trials is very slow and there is a very low conviction rate because in most of the cases, in such a long period of time, the witnesses deny to come out of fear and in some cases, the pieces of evidence are lost.

- **Lack of coordination**

Lack of synergy between law enforcement and legislative bodies enables criminals to exploit loopholes and capitalise on demand for illicit commodities. In some cases, controls and regulatory frameworks have themselves proved to be criminogenic.

- **Economic disparity**

This will bring individuals into greater proximity to organised crime. Poverty, in some cases aggravated by the global economic crisis, has the potential to swell the workforces of criminal groups. Projected food crises and other disruptions to supply chains will also fuel markets for counterfeit and stolen goods.

- **Emerging markets**

Emerging markets such as alternative energy supply and infrastructure, trade in rare minerals and the disposal of toxic waste. etc criminal groups will continue to spot opportunities in such markets in which there are large incentives, and which are not subject to sufficient scrutiny or competition

from legitimate investors. One example of this is the alleged contribution of metal theft to fluctuating metal prices.

- **Development of the Internet and related technologies**

This will not only put new tools at the disposal of all criminal groups, but will also expose new vulnerabilities in our information society. A future convergence of "entry level" criminal tools and a new generation of technically capable youth raises the possibility of online petty crime. In addition, there is an increasing overlap between organised crime and terrorist activity on the Internet.

Terrorism

International terrorism: Violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations (state-sponsored).

Domestic terrorism: Violent, criminal acts committed by individuals and/or groups to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature.

Types of Terrorism

- **Ethno-Nationalist Terrorism**

Ethnic terrorism can be deliberate

violence by a subnational ethnic group to advance its cause. Such violence usually focuses either on the creation of a separate State or on the elevation of the status of one ethnic group over others. Tamil Nationalist groups in Sri Lanka and insurgent groups in North East India are examples of ethno-nationalist terrorist activity.

- **Religious Terrorism**

In this the practitioners of terrorism motivated either in whole or in part by a religious imperative consider violence as a divine duty or a sacramental act. It embraces different means of legitimization and justification compared to other terrorist groups, and these distinguishing factors make religious terrorism more destructive in nature.

- **Ideology Oriented Terrorism**

Any ideology can be used to support the use of violence and terrorism. Ideology oriented terrorism can be seen through Left-wing and Right-wing terrorism.

- **Narco-terrorism**

Narco-terrorism as a means of terrorism or at any rate as a means of funding terrorism. Narco-terrorism combines two criminal activities; drug trafficking and terrorist violence. Narco-terrorism is motivated mainly by economic reasons as it helps the terrorist organizations raise huge sums of money with minimum cost for their activities.

Challenges in controlling the terrorism

India specific

- Hostile neighborhood which is breeding ground for terrorism
- Lack of citizen participation and private sector participation in beefing up the security apparatus
- absence of "bottom up" security architecture.
- Weak coordination between various security agencies.
- Presence of anational element and insurgent group.

Global level

- **Narrow Global War on Terrorism (GWOT):**

The first challenge is that the "Global War on Terrorism" (GWOT), as it was conceived by a post 9/11 United States is over with the withdrawal of USA from Afganistana, as the United States negotiated with the Taliban, and then withdrew from Afghanistan.

- **Divided UN security council**

In polarised world devided opinion in security council regarding affects fight agains terrorism.

- **Toothless FATF**

The decision of FATF mostly affected by geopolitical trends around the world.This affect counterterrorism efforts negatively at global level.

- **Linkages with organized crime**

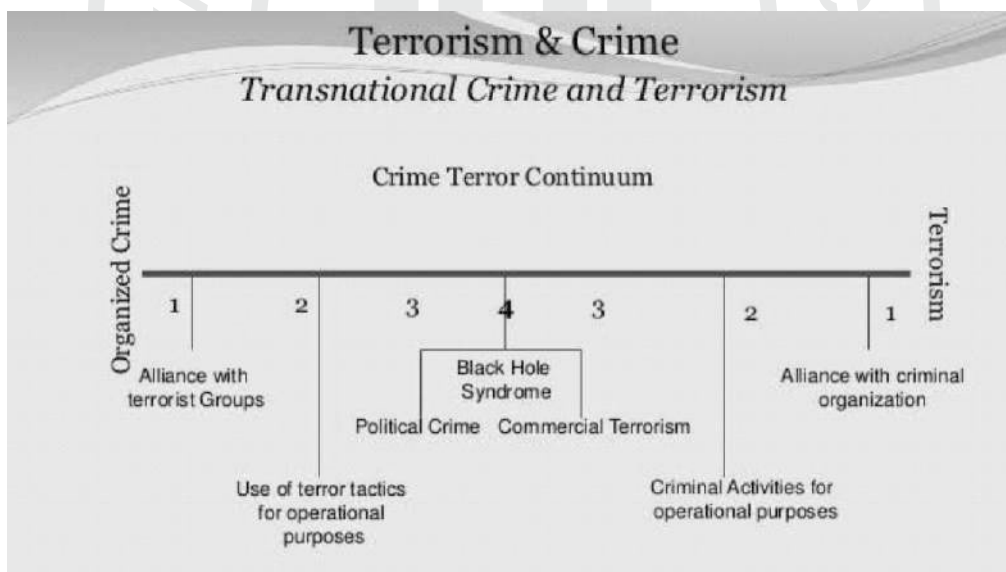
We are going study detail about this topic under separate heading

How organized crime and terrorism link with each other

Introduction

Terrorism is another form of "organized" criminal behaviour, but it is distinct from organized crime. In general terms, terrorism involves crimes committed with the objective of intimidating a population or compelling a government or international organization with a view to achieving political or social objectives.

The linkage can be seen through following diagram



Linkage

- **Source of financing**

Terrorist group can benefit from the illicit trade in natural resources and wildlife, the abuse of legitimate commercial enterprise, donations, and proceeds of criminal activity, including kidnapping for ransom, extortion and bank robbery, as well as piracy. All these activity related to organised crime

Examples

- In J&K, counterfeit currency has been a major source of funding for terrorism.
- In the Northeast, extortion is the fundamental basis for funding all forms of terrorism.
- **Logistic Support**
Terrorist group get logistic support through illicit trafficking of arms and ammunition, persons and drug all these directly helps in terrorist activity.

Examples

- Arms Trafficking by Maoist insurgent on Nepal india border from criminal syndicates
- Arms and explosive delivery through drone by arms trafficker on LOC.
- **Technological Support**
Organised crime like cybercrime provides technological support to terrorist group
- **Common motive**
Sometime both terrorist and organised crime syndicate work for common motive. That common motive is instability in any particular region. This instability helps terrorist group to achieve social and political goal whereas instability creates weak security architecture in that particular region this helps organised crime to earn more profit.

Efforts to Curb menace of linkage between organised crime and terrorism

Global level

- Security Council adopted resolution 2482, which urged Member States to address the links between organised crime and terrorism.
- Creation of financial action task force (FATF) to deal with issue of money laundering and terror funding.
- UNODC (United Nations office on Drug and crime) supports efforts to tackle link between organized crime and Terrorism. These efforts includes initiatives on improving border management, such as profiling high-risk passengers and cargo, on facilitating international cooperation, and on combating the financing of terrorism.

India Specific

- Enactment of Maharashtra control of organised crime act, 1999.
- Narcotic Drugs and Psychotropic Substances Act, 1985.
- National Investigation Agency Act 2008
- Laws under IPC and crpc to control unlawful activity.

Way Forward

- Technology, Manpower, and intelligence must work together to counter organized crime and terrorism.
- There is a need for fine-tuning of the criminal investigation so as to find and establish links of a crime syndicate with terrorism.
- Developing Common strategies to tackle with emerging threat from linkage of organised crime and terrorism.

- More robust international coordination is necessary to tackle nexus of organized crime and terrorism.
- India must continue to engage the international space for better policy, concerted actions against state-sponsored terrorism, and terrorist financing.



Various Security Forces, Agencies And Their Mandate

First of all let us see the past year UPSC questions and understand their demand.

Questions	Keyword/Context/Demand
Human right activists constantly highlight the view that the Armed Forces (Special Powers) Act, 1958 (AFSPA) is a draconian act leading to cases of human rights abuses by the security forces. What sections of AFSPA are opposed by the activists? Critically evaluate the requirement with reference to the view held by the Apex Court. (2015, 12.5 Marks)	AFSA and human right abuses, Critically Evaluate

Introduction

The various Security forces of the Union of India have separate mandates and are handled by different ministries. The majority of the external security threats in India are managed by the Ministry of Defence with the help of the Ministry of Home Affairs. Most of the internal security challenges and their management in border areas are also handled by both the Defence Ministry and the Home Ministry. Internal security threats such as insurgencies, separatism and riots etc are the primary responsibility of the Ministry of Home Affairs.

The various Security forces

Under Defence Ministry

Security Force and it's Mandates	Overall Issue associated with all 3 wings of Indian armed forces
<p>Indian Army</p> <ul style="list-style-type: none"> • Indian Army (IA) is committed to the defence of the country from external and internal threats across the entire spectrum of warfare. • Indian Army also provides aid during disaster situations through various operations like Operation Surya Hope (Uttarakhand floods, Kerala Flood In 2018). • Government of India also contributes its army personnel for United Nations peace making operations in different countries. 	<ul style="list-style-type: none"> • At present, military planning is hamstrung by lack of a clearly articulated and integrated military strategy. • Lack of modernisation and an alarmingly large percentage of old equipment are still in use because several proposals for acquisition of new equipment and upgradation of existing equipment having been inordinately delayed. • There seems to be an expanding hollowness in arms and ammunition over the years due to quality issues related to indigenous production of modern ammunition, compounded by inadequate budgetary support.

<p>Indian Air Force</p> <ul style="list-style-type: none"> • The Indian Air Force, similarly, aims to overwhelm the adversaries with application of aerospace power in defence of the nation. The Union War Book mandates the Indian Air Force as being the sole agency responsible for air defence of the Indian airspace. • With Air Defence elements being provided to Army and Navy as well, seamless integration and free flow of information is an inescapable need 	<ul style="list-style-type: none"> • Lack of capital budget for new procurement schemes, especially 'big ticket' items, is another challenge. This is due to the fact that there has been inadequate allocation of defence budget for several years now. Though at least 2.5 percent of GDP should be allotted for defence expenditure (other than pension), only 1.5 to 1.7 percent is actually allotted, resulting in reduction of budget allocation in real terms after taking into account the annual inflation component
<p>Indian Navy</p> <ul style="list-style-type: none"> • The Indian Navy is responsible for full range of operations in which a nation's naval forces may be involved is vast, ranging from high intensity war fighting at one end to humanitarian assistance and disaster relief operations at the other end. • Its major objective is Security of India's territorial integrity, citizens and offshore assets from sea-borne threat. 	<ul style="list-style-type: none"> • There is not enough expertise within the Army in the field of weapon design and technology, resulting in lack of meaningful inputs for the indigenous defence industry. • Faulty human resource policies in the Army in recent years, which have incentivised holding more manpower. This faulty human resource policy has sucked up a large percentage of the revenue budget of the Armed Forces without proportionate returns in 'capability' terms
<p>Indian Coast Guard</p> <ul style="list-style-type: none"> • The Indian Coast Guard was established in 1978 by the Coast Guard Act, 1978 as an independent Armed force of India. <p>Duties Of Indian coast guard</p> <ul style="list-style-type: none"> • Safety and Protection of Artificial Islands and Offshore Terminals • Protection of Fishermen • Assistance to Fishermen in Distress at Sea • Preservation and Protection of Marine Environment • Prevention and Control of Marine Pollution • Assisting the Customs and other authorities in anti smuggling operations • Enforcement of Maritime Laws in Force 	

Under Home Ministry

CAPF

Central Armed Police Forces (CAPF) is the collective name of central police organisations in India under the Ministry of Home Affairs (MHA). These are technically paramilitary forces formerly known as Central Paramilitary Forces (CPMF). Since 2011, India adopted the term "central armed police forces" to drop the word "paramilitary". These forces are responsible for internal security and guarding the borders.

CAPF comprises following central police forces we can study their mandates and issues associated with these forces in tabular form.

Security Force & it's Mandates	Cumulative issues of all Central Security forces.
<p>Assam Rifles (AR)</p> <ul style="list-style-type: none"> • The Assam Rifles came into being in 1835, as a militia called the 'Cachar Levy', to primarily protect British Tea estates and their settlements against tribal raids. • This Force significantly contributed to opening the region to administration and commerce and over time they came to be known as the "right arm of the civil and left arm of the military". • AR guards India's international border with Myanmar. 	<ul style="list-style-type: none"> • Deployment of CAPFs: There is heavy dependence of states on central armed police forces (CAPFs), even for everyday law and order issues. This affects the anti-insurgency and border guarding operations, besides curtailing the training needs of these forces. • Training of CAPFs: There is an urgent need to update the curriculum and infrastructure in training institutes for CAPFs. • Huge Vacancy in six Central Armed Police Forces (CAPFs). • Promotion of CAPFs: The top positions in CAPFs are occupied by IPS officers. This has a demoralising effect on the officers of the CAPFs, and impacts the effectiveness of the forces.
<p>Border Security Force (BSF)</p> <ul style="list-style-type: none"> • The Border Security Force (BSF) is a Border Guarding Force of India. • The BSF is the border guard of the country and is called the 'India's First Line of Defence'. • This force came into being in the wake of the 1965 Indo-Pakistan war. It was established on 1st December 1965. • It is a paramilitary force charged with guarding India's land border during peacetime and preventing transnational crime. • It is a Union Government Agency under the administrative control of the Ministry of Home Affairs. It is one of many law enforcement agencies of India. • BSF guards India's international border with Pakistan and Bangladesh. 	<ul style="list-style-type: none"> • In addition, there is frustration in CAPFs due to stagnation in promotions and lack of cadre review. • Poor Working Conditions: It is observed that they had to work 16-18 hours a day, with little time for rest or sleep. The personnel are also not satisfied with medical facilities that are being provided at border locations. • Lack of intelligence gathering mechanism. • Lack of a reliable internal grievance procedure. Some CAPF soldiers have been posting complaints on social media and disobeying instructions because the force's grievance process is inadequate.
<p>Central Industrial Security Force (CISF)</p> <ul style="list-style-type: none"> • The CISF came into existence in 1969 with a modest beginning, having three battalions, to provide integrated security cover to the Public Sector Undertakings (PSUs). • With globalization and liberalization of the economy, CISF is no longer a PSU-centric organization. Instead, it has become a premier multi-skilled security agency of the country, mandated to provide security to major critical infrastructure installations of the country in diverse areas. 	<ul style="list-style-type: none"> • Increased political influence has eroded the chain of command. Senior officers are quite often not able to transfer or punish delinquent junior officers because of their political linkages.

- CISF is currently providing security cover to nuclear installations, space establishments, airports, seaports, power plants, sensitive Government buildings and ever heritage monuments.
- Among the important responsibilities recently entrusted to the CISF are the Delhi Metro Rail Corporation, VIP Security, Disaster Management and establishment of a Formed Police Unit (FPU) of the UN at Haiti.

Central Reserve Police Force (CRPF)

- The Central Reserve Police Force came into existence as Crown Representative's Police on 27th July 1939. It became the Central Reserve Police Force on the enactment of the CRPF Act on 28th December 1949.
- The mission of the Central Reserve Police Force is to enable the government to maintain Rule of Law, Public Order and Internal Security effectively and efficiently, to Preserve National Integrity and Promote Social Harmony and Development by upholding the supremacy of the Constitution.

Indo Tibetan Border Police (ITBP):

- ITBP was raised on 24 Oct 1962.
- Presently, ITBP is deployed on border guarding duties from Karakoram Pass in Ladakh to Jachep La in Arunachal Pradesh covering 3488 km of Indo-China Border and manning Border Outposts on altitudes ranging from 9000' to 18700' in the Western, Middle and Eastern sectors of the Indo-China Border.
- ITBP is a specialized mountain force and most of the officers and men are professionally trained mountaineers and skiers.
- Being the first responder for natural disasters, ITBP has been carrying out numerous rescue and relief operations across the country.
- ITBP guards India's international border with China.

Sashastra Seema Bal (SSB):

- The Special Service Bureau (now Sashastra Seema Bal) was thus conceived in November 1962 and eventually created in March 1963.
- The sole objective of achieving 'Total security prepared-ness' in the remote border areas for performing a 'stay-behind' role in the event of a war.
- SSB is now spread along the International border across Uttarakhand, UP, Bihar, West Bengal, Sikkim, Assam and Arunachal Pradesh.
- Other duty assigned by the Central Government to SSB are being deployed for Law & Order, Counter Insurgency Operations and Election duty.
- SSB guards India's international border with Nepal and Bhutan.

Other Security forces and their Mandates.

Security Force	Mandates
Railway Protection Force (RPF)	<ul style="list-style-type: none"> • Railway Protection Force (RPF), ensures the safety and security of travelling public in the Railways. • It is under the Ministry of Railways. They protect railway passengers, Station area and railway property. • They take care of criminals and antisocial elements from trains, railway premises and passenger area. • This is the only armed force of the Union which has the power to arrest, investigate and prosecute criminals
National Disaster Response Force (NDRF)	<ul style="list-style-type: none"> • The Disaster Management Act has statutory provisions for the constitution of National Disaster Response Force (NDRF) for the purpose of specialized response to natural and man-made disasters. • Accordingly, in 2006 NDRF was constituted with 8 Battalions. At present, NDRF has a strength of 12 Battalions. It works under the Ministry of Home Affairs. • It is manned by persons on deputation from various CAPFs and also re-employs physically fit members of the armed forces who have retired but are still under reserve liability. <p>Role</p> <ul style="list-style-type: none"> • Quick response during disasters. • Acquire and continuous updating of its own training and skills. • Community Capacity Building Programme. • Immediate deployment during impending disaster situations. • Impart basic and operational level training to State Response
Special Protection Group (SPG)	<ul style="list-style-type: none"> • After the assassination of PM Indira Gandhi, the government felt a need to raise a dedicated force whose sole responsibility will be to protect present and former PMs of India and their immediate family members. • Thus in 1988 SPG was established. Special Protection Group or SPG as it is known is a finely trained organization which provides proximate security to the VIPs of India. • The Special Protection Group (SPG) under the Cabinet Secretariat is also classified as a CAPF. • It works under the control of the Cabinet Secretariat.

Various law enforcement agencies and intelligence agencies of India.

Intelligence Agency	Mandates
Research and Analysis Wing (R&AW)	It gathers information about counter-proliferation, foreign intelligence and counter-terrorism and advises Indian policymakers, and advances India's foreign strategic interests.
Intelligence Bureau (IB)	It is a domestic internal security and counter-intelligence agency of India.
Central Bureau of Investigation (CBI)	Investigate bribery and governmental corruption and also investigate breaches of central laws enforceable by GOI, multi-state organised crime, and multi-agency or international cases.
Computer Emergency Response Team (CERT)	Deals with cyber security threats like hacking and phishing. It strengthens the security-related defence of the Indian Internet domain.
Wildlife Crime Control Bureau (WCCB)	Deals with organised wildlife crime in India
National Investigation Agency (NIA)	countering terrorism
National Technical Research Organisation (NTRO)	Responsible for geospatial intelligence and satellite imagery and provides technical intelligence to other agencies
Serious Fraud Investigation Office (SFIO)	Conducts multi-disciplinary investigations of major corporate frauds.
Defence Intelligence Agency (DIA)	Provides and coordinates defence and military intelligence to the Indian Armed Forces.
National Crime Record Bureau (NCR)	Functions as a repository of information on crime and criminals to help assist the investigators in linking crime to the perpetrators.
Narcotics Control Bureau (NCB)	Combats drug trafficking and the use of illegal substances as per the provisions of the NDPS Act

Need of Reforms

1. Armed force reforms

Shekatkar Committee recommendation

- Defence budget: The panel has recommended a roll-on defence budget to have enough capital expenditure available for modernisation as against the present practice of surrendering unspent capital budget at the end of each financial year.
- Transparency: The committee has recommended a performance audit of the role of non-combat organisations under the Defence Ministry.

- **Manpower:** The committee has suggested downsizing or rationalisation of manpower in these organisations, which can lead to significant savings.
- Another recommendation is the setting up of a joint services war college for training middle-level officers.
- **NCC reforms:** Comprehensive reforms in the running of NCC could be rolled out over the next few years.
- Progressively, the NCC could be run by re-employed or on-contract ex-service personnel.

2. CAPF Reforms

- Moreover, given the evolution of hybrid warfare, the contents of training should be a mix of conventional matters as well as latest technologies such as ICT, and cyber security
- **Corrective Measures in Cadre Policy:** Citing the dissatisfaction in Cadre policy, **Joshi Committee** recommended that top positions should be filled from the respective cadre of the CAPF.
- **Personnel Reforms:** Workshops on stress management should regularly be undertaken, and yoga and meditation be made part of the daily exercise for CAPF personnel.
- Further, the provision of accommodation near the deployment of the respective force, to enable personnel to meet their family members, can also be explored.
- Government should improve CAPF's infrastructure capabilities in areas like AI, cyber security, drones, and other technologies through technology infusion. Private enterprises and research institutions like DRDO should be supported for this.
- Procurement bottlenecks should be located and fixed. Negotiations between the Ministry of Home Affairs and CAPFs and ordnance factories and manufacturers, whether in the public or private sector, are necessary to guarantee a continuous flow of supplies for tools and other infrastructure.
- Information exchange across agencies should be synchronised, and there should be no delays in acquiring intelligence.

3. Police Reforms

In Prakash Sing case in 2006 SC gave following Directives on Police Reforms

- Constitute a state security commission to make sure that the state does not exercise undue influence on the police.
- The DGP should be appointed a transparent and merit-based process and have a minimum tenure of two years.
- Set up National security commission at Central level.
- Set up police complete authority at state and district level.
- Set up Police establishment board.

NITIAayog suggested the following reforms

- States should be encouraged, with fiscal incentives, to introduce 'The Model Police Act of 2015' as it modernises the mandate of the police.

- A Task Force must be created under the MHA to identify non-core functions that can be outsourced to save on manpower and help in reducing the workload of the police.
- The states should be encouraged to ensure that the representation of women in the police force is increased.
- Moving police as well as public order to the Concurrent List to tackle increasing inter-state crime and terrorism under a unified framework.

Women in armed forces

Introduction

- The Supreme Court, in a landmark decision on February 17, 2020, ordered that women officers in the Army be given permanent commissions.
- It rejected the Centre's claim, that their physiological limits were based on "sex stereotypes" and "gender discrimination against women."
- In 2021, the apex court had authorised women to take the National Defence Academy entrance exams (NDA).

Significance

- Women officers will be given equal opportunity to contribute to the nation's Security.
- It is an important step towards gender equality in the armed forces.
- It provides women with a more challenging and fulfilling career.
- It will help to change the "regressive mindset" for not allowing women in the armed forces.

Challenges

- Military's perception that it would lead to "operational, practical and cultural problems".
- Officers in combat branches have to fight together, there is no privacy.
- It's tough to maintain proper living conditions for women in combat situations, especially given social norms in India.
- The challenge for women officers to meet the hazards of service owing to their prolonged absence during pregnancy, motherhood and domestic responsibilities.
- The high standards of physical fitness are required for a long period.
- Fear factor of being captured by the enemy and its consequences.

Way Ahead

- The Armed Forces must take a proactive approach themselves in ensuring gender equality rather than waiting for courts to intervene.
- As women get ready to stride into the combat corps, they may need to combat attitudinal hurdles.

Though this topic has not asked much in UPSC, don't ignore this topic.



PRAYAAS - Daily Answer Writing (UPSC)

FREE ANSWER WRITING INITIATIVE



- Open to all Sincere aspirants.
- Monday to Friday Daily Answer Writing Practice.
- Detailed Individual and Group Feedback.
- Model Answer will be provided both in English and Marathi on Daily Basis.
- Available both in Marathi and English.
- Planned Syllabus Coverage.
- Immediate evaluation within 24 hours.
- Exam oriented Evaluation and Feedback.
- Personal counselling regarding Answer Writing through expert faculty.

Scan the QR code to join us on YouTube and telegram



Address :
Ramashree, CTS No, 279, NC Kelkar
Road, Narayan Peth Pune.