

GS MAINS CLASSES

BASIC TO ADVANCE

**ADVANCE
CLASS NOTES**

INTERNAL SECURITY

GS SCORE

An Institute for Civil Services

GYAN CAPSULES

YOUR BOOSTER DOSE

PRELIMS FACT FILE



**2+ YEARS PRELIMS
CURRENT AFFAIRS TESTS**



**ALL INDIA OPEN
MOCK TEST**



7+ YEARS UPSC PYQ



PIB COMPILATION



GS ANALYST:
Daily **CURRENT AFFAIRS**



NCERT REVISION TESTS



SCAN QR CODE TO REGISTER / DOWNLOAD



1B, Second Floor, Pusa Road, Karol Bagh,
New Delhi - 110005 (Beside Karol Bagh
Metro Station Gate No. 8)



8448496262



iasscore.in

Contents

1.	INTERNAL SECURITY OF INDIA 01-04	
	(AN OVERVIEW)	
	▢ Background & Evolution	1
	▢ Internal Security Challenges	2
	▢ Factors responsible for threats and steps needed	4
	▢ Ajit Doval on Internal Security of India	4
2.	DEVELOPMENT & EXTREMISM..... 05-30	
	▢ Terrorism Threat to India	5
	▢ NAXALISM.....	9
	▢ Insurgency in North-East	16
	▢ Kashmir Issue	21
	▢ The Khalistan Movement	23
	▢ De-Radicalization in India.....	24
	▢ Communal Violence.....	25
	▢ Mob Violence.....	27
	▢ Armed Force Special Power Act (AFSPA).....	28
	▢ Bio-Terrorism.....	30
3.	ORGANISED CRIME..... 31-37	
	▢ Terror Financing.....	35
	▢ Drug Trafficking	36

4.	MONEY LAUNDERING 38-46 & BLACK MONEY	
	❑ Black Money in India	43
5.	CYBER SECURITY..... 47-63	
	❑ Cyber Threats.....	47
	❑ Challenges in Cyber Security.....	51
	❑ Information Technology (IT) Act 2000	56
	❑ National Cyber Exercise (NCX)	58
	❑ National Security Council (NSC)	58
	❑ International Measures	59
	❑ Paris Call	59
	❑ Internet Governance Forum (IGF)	60
	❑ Council of Europe.....	60
	❑ ICANN	60
	❑ United Nations (UN)	60
	❑ Cyber Warfare	61
6.	ROLE OF MEDIA AND SOCIAL..... 64-74 NETWORKING SITES IN INTERNAL SECURITY CHALLENGES	
	❑ Role of media in internal security challenges.....	64
	❑ Role of social media in internal security challenges	67
7.	ISSUES RELATED..... 73-92 TO SECURITY FORCES	
	❑ Central Armed Police Forces.....	73
	❑ Police Reforms	76
	❑ Police Reform with Respect to Cyber Security	77
	❑ Need for reforms in the country's Intelligence Apparatus	78
	❑ Coastal Security	80
	❑ India's Dominance in Indian Ocean Region.....	81
	❑ Need for a National Maritime Security Coordinator (NMSC)	82
	❑ Border Area Issues of India with all the neighbours	83

❑ China's work on railway up to Arunachal border	86
❑ Government implements Shekatkar Committee recommendations related to creating border infrastructure	87
❑ Issues with Armed Forces	87
❑ National Maritime Security coordinator.....	88
❑ Infrastructure Development in Border Areas	89
❑ High altitude pseudo-satellites (HAPS).....	90
❑ Security threats posed by drones	91

8. DEFENCE PROCUREMENT 93-100

❑ Working Analysis of Defence PSU	93
❑ Defence Research and Development Organisation (DRDO).....	94
❑ Hindustan Aeronautics Limited	95
❑ Atmanirbhar Bharat	96
❑ Technological Dependence on Other Nations.....	97
❑ Decoupling India's Manufacturing with China.....	98
❑ Modernisation Fund for Defence and Internal Security (MFDIS).....	99
❑ Defence Production and Export Promotion Policy 2020.....	100

9. MILITARY POLICIES ACROSS 101-106 THE GLOBE

❑ Nuclear Arms race Issues.....	101
❑ India's Soft Power	102
❑ Open Skies Treaty	103
❑ Women into Military Police.....	104
❑ Integrated Battle Groups	105

INTERNAL SECURITY OF INDIA (AN OVERVIEW)

The emerging security environment is fundamentally different from what it was a couple of decades ago. There are national and transnational players who are on the lookout to exploit the in the internal and external security structure of a nation. Asymmetric means and hybrid threats can destabilise a nation not in years, but in months and weeks.

India is facing multidimensional security challenges from separatist and secessionist movements that have taken root due to socio-political discrimination and religion-based radicalisation. The social media and cyber war has made the situation more complex and challenging, by providing the means for the integration of state and non-state actors for common objectives. The active support to some of these movements by inimical forces is further complicating the overall security environment. These threats are ultimately resulting in physical, cultural and structural violence that allows no space for dialogue and reconciliation. The struggle primarily is for control over resources, spread of ideologies and creation of ethno-religious transnational states.

Background & Evolution

In the Arthashastra, Kautilya wrote that a state could be at risk from four types of threats:

Internal

External

Internally aided external

Externally aided internal

He advised that of these four types, internal threats should be taken care of immediately, for internal troubles, like the fear of the lurking snake, are far more serious than external threats. The most dangerous enemy is the enemy within.

The long struggle with the British and the arduous efforts to consolidate British provinces and Princely states into a federal India generated considerable anxiety about sustainability of Indian state, particularly when the country was marked by numerous ethnic groups, varied culture, innumerable languages, multitude of religion, castes and tribes, etc. It was a challenging task for the constitution makers to build the effective institutions and constitutional framework in this regard.

The Republic of India took the challenge of internal security with all earnestness. The Constitution of India envisaged a federal framework of polity with clear demarcation of powers entrusted to the Union and the Units in the Seventh Schedule of the Constitution. It is noteworthy in this context that the Constitution allotted public order and police to the States and put criminal law, criminal procedure, preventive detention, etc. in the concurrent jurisdiction in view of their relevance to the Centre's responsibility for national security and the need to maintain uniformity of criminal law and procedure across the country.

For extraordinary situation which demand extraordinary interventions, Article 352 was provided which dealt with the 'Emergency Situation'— A potential bearer on Internal Security as felt by our forefathers. Similar provisions were provided in other articles. Article 352, constitutional break-down of state machinery under Article 356 and financial emergency under Article 360 provided such possibilities.

Article 355 empowers the Union Government to deploy central paramilitary forces in a state where public order is in jeopardy and outside the control of the police as it shall be the duty of the Union to protect every State against external aggression and internal disturbance. Article 257 (1) provides that in case of conflict, the valid exercise of Union executive power must take priority over the valid exercise of state executive power.

Then, came The 42nd Amendment to the Constitution (1976), which inserted in the Union list "Deployment of any armed forces of the Union or any other force subject to the control of the Union or any contingent or unit thereof in any State in aid of the civil power; powers, jurisdiction, privileges and liabilities of the members of such forces while on such deployment". The State list was also altered to make additions to 'Public Order' and 'Police'.

The Constitution also carried a strong centralist thrust and enabled. Thus, the internal security challenges were visioned at the very outset and there were provisions to deal with it, but sadly, because of the last three decades witnessing multiple violence in different part of country, posing internal security threats, it was perceived to make several laws which could provide measures to deal with them. They were: Jammu and Kashmir Public Safety Act, 1978, Assam Preventive Detention Act, 1980, National Security Act, 1980, amended 1984 and 1987. Anti-Hijacking Act, 1982, Armed Forces (Punjab and Chandigarh) Special Powers Act, 1983, to just name a few.

Thus, it may be seen that India's readiness to deal with the internal security challenges witnessed organic growth, and was continuous in the sense that, after independence, several measures were taken by Government, Policy makers and Strategic thinkers in this direction.

Internal Security Challenges

Terrorism/Militancy: Terrorism is the calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. Within this definition, there are three key elements violence, fear, and intimidation and each element produces terror in its victims.

Left wing extremism: Left-wing extremists adapt their political activities to revolutionary Marxist or anarchist ideas, and they endeavour to replace the existing political and social order with a socialist or communist system or an anarchist society "free of rule". To this end, they participate in social protests, and they attempt to instrumentalize them for their purposes. Their forms of action range from open agitation to clandestine, partly serious acts of violence, with isolated autonomous groups also accepting individuals to be injured.

Communal divide: Islamist fundamentalist organizations rooted in religious obscurantism have long been prone to sudden bursts of irrational violence at the slightest provocation. These organizations initiate communal violence.

Organized crimes: Organized crime is defined as "those involved, normally working with others, In

continuing serious criminal activities for substantial profit, else where". The co reorganized crime activity is the supply of illegal goods and services to countless numbers of citizen customers. It employs illegitimate methods-monopolization, terrorism, extortion and tax-evasion to drive out or control lawful ownership and leadership, and to extract illegal profits from the public.

Border Security: Border security is aimed at securing nation's borders against interests hostile to the nation by putting in place processes to interdict them and facilitate legitimate trade. The external forces utilize the border dispute for infiltration and posses challenge for internal security.

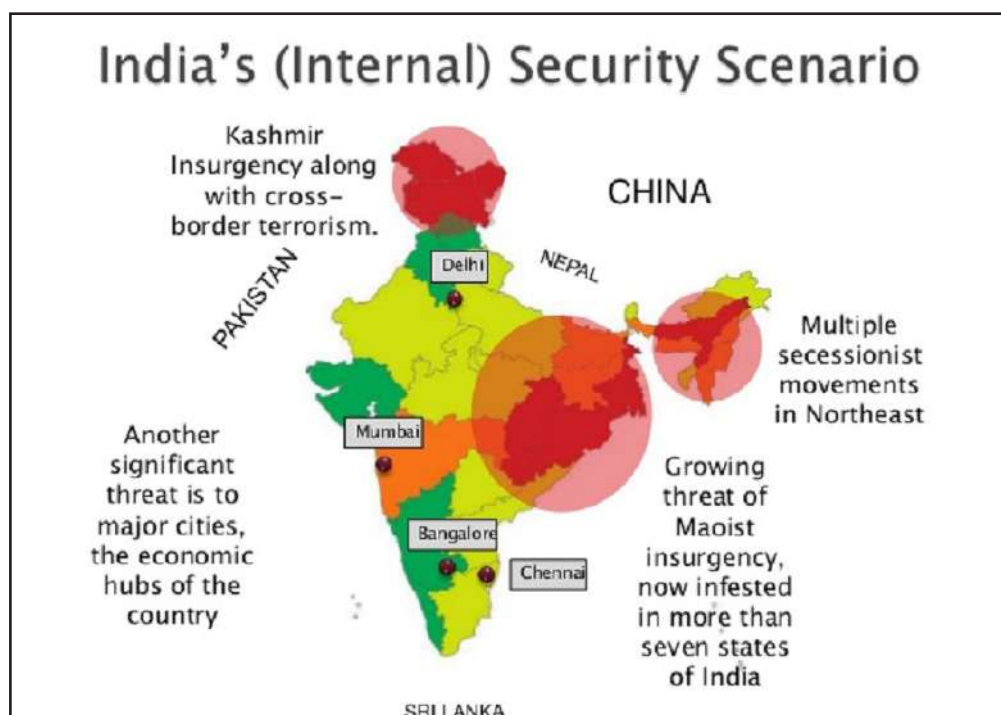
Cyber crime: Cyber-crime encompasses any criminal act dealing with computers and networks. These include cyber harassment, cyber stalking, cyber terrorism, cyber warfare, etc.

Illegal immigration: It is note as for the people to obtain valid travel documents and jobs abroad, they fall into the trap of unscrupulous travel agents and employment agencies. These agencies promise to give them valid travel documents and employment abroad on the payment of huge amounts. Often the travel documents are not valid, and sometimes they are simply dumped into foreign lands without giving them the promised employment and treated as illegal migrants.

Smuggling and traffcking: It is perhaps the most serious organized crime affecting the country and is truly transnational in character. India is geographically situated between the countries of Golden Triangle and Golden Crescent and is a transit point for narcotic drugs produced in these regions to the West. India also produces a considerable amount of licit opium, part of which also finds place in the illicit market in different forms.

Hawala transfers (illegal money transfers): Illegal currency transfers via non banking channels are called Hawala. It is an underground banking system. Secret flows of money can take place in free currency areas as well as in areas where currency conversion restrictions are practiced due to the shortage of foreign exchange. This leads to tax evasion.

Economic Security: The growing convergence of economies and their integration into the process of globalization have led to the proliferation of platforms of collaboration and coordination for sharing of knowledge, skills, market and technology in order to stay competitive. This has led to considerable accretion in the numbers of players across cultures and faiths at different levels, exposing the economy to threats of espionage, subversion, theft, physical attack and accident. This has encouraged trans-border migrations, posing new challenges to Immigration and Border and Coastal Security Management.



Factors responsible for threats and steps needed

Political reasons such as the threat in form of secessionist, separatist or even regional in nature.

Socio-economic factors are also at the back of many movements which are big threats to the internal security of the country. Equitable growth and development is the spirit of our constitution. Therefore, we have to ensure that development reaches all sections of the society and there are no regional disparities.

Lack of good governance also strengthens the hands of anti-establishment elements, who pose a challenge to the internal security of the country. Such elements take advantage of mismanagement and corruption in government schemes, poor implementation of laws and absence of government machinery in the remote areas.

Lack of reforms in Police & security forces: Police needs to be sensitized so that it becomes people friendly. Other security forces aiding state police need to coordinate with the state police and help achieve overall goal of maintaining the internal security.

The capability of the state police is limited as far training and equipment are concerned. Central government agencies have started capacity building over the last years but still there is scope for improvement. As of now, for operations, IB plays the role of the coordinator with the police of different states but if operations need to be carried out simultaneously in many states, there is no unified command. Also some states do not have a desirable capability. Therefore there is need for central agency to coordinate operations to all over the country, but this agency should work in coordination with the state police and not independently.

Lack of centre state coordination also leads to many problems related to internal security. This coordination problem exists in all areas from intelligence to operations. We need to develop an institutional framework which resolves all these centre-state coordination problems and ensure synergy at all levels.

Criminal justice system is very sluggish and a lot of time is spent in procedural aspects. There should be a time bound justice system. Special fast track courts should be established for quick disposal of terrorist cases. There is need to improve a lot in this direction.

Ajit Doval on Internal Security of India:

You cannot have a great powerful country if you cannot manage its internal security.

You have to master the technology. The biggest challenge will be now if you have to fight and win this fourth generation of warfare, whether it is organised crime, terrorism, insurgency or foreign powers trying to meddle into your internal affairs you have got to be demonstrative.

Now it is a war of a policeman, as civil society is mostly affected. If you win, the country wins. Many countries are collapsing with internal security problems. Only police can fight and win the battle

You are now in the phase of fourth generation war and this is a very, very difficult war. It is a warfare with an invisible enemy... it's a warfare, in which the civil society is both the battleground and the ground and the people that you have to protect.

DEVELOPMENT & EXTREMISM

Terrorism Threat to India

Terrorism in India, according to the Home Ministry, poses a significant threat to the people of India. Compared to other countries, India faces a wide range of terror groups. Terrorism found in India includes extremism/fundamentalism based terrorism, separatist terrorism, left wing terrorism, right wing terrorism, etc.

Classification of Terrorism

- ❑ Terrorism can be classified into two categories:
 - Terrorism by external state actors and
 - Terrorism by non-state actors.

Terrorism by External State Actors

- ❑ State terrorism refers to acts of terrorism which a state conducts against another state or acts of terrorism which a state conducts against its own citizens. Examples of state terrorism include the police state measures employed by the Soviet Union beginning in the 1930s and by Germany's Nazi regime in the 1930s and 1940s. Another example-The US launched the Global War on Terror (GWOT) primarily targeting Al Qaeda but subsequently supported and armed Al Qaeda in Bosnia and Libya, and is doing so similarly in Syria and Iran.
- ❑ Terrorism by Non-state Actors: In this case, the act of terrorism is performed by an individual or a group which is neither associated with nor financed by any Government. Non-state actors generally don't have direct or indirect link with any government or government agency while pursuing their agenda, though indirect link cannot be completely ruled out. Naxalites, LTTE and North-east extremists are some examples of non-state actors. Many important terrorist groups like the Lashkar-e-Taiba (LeT) and the Indian Mujahideen (IM) also claim to be non-state actors, but have de-facto support from Pakistan.

Causes of Terrorism/ Roots of Terrorism:

- ❑ Political Terrorism - The grievances against a certain political policy or lack of political participation in states may be of reason to join or form terrorist groups. The Left and right wing terrorists are the

example of this type of terrorism. It is akin to ethno-nationalist terrorism, but in this, the demand is not to create new state but to change the political policy within the nation.

- ❑ Strategic - Saying that a group has a strategic cause for using terrorism is that another way of saying that terrorism isn't a random, but it is a chosen tactic for a larger goal. Hamas, for example, uses terrorist tactics, but not out of a random desire to fire rockets at Israeli Jewish civilians. Instead, they seek to leverage violence (and cease-fires) in order to gain specific concessions related to their goals vis-a-vis, Israel and Fatah.
- ❑ Religious - Experts began to argue in the 1990s that a new form of terrorism fueled by religious fervor was on the rise. They pointed to organizations such as Al Qaeda, Aum Shinrikyo (a Japanese cult), and Christian identity groups. Religious ideas, such as martyrdom, were seen as particularly dangerous.
- ❑ Poverty and Economic Problems: The more important factor of terrorism is disparity in the distribution of resources. This is a main cause of terrorism.
- ❑ Anti Democracy: The democratic government represents the people and provides political means to voice against grievances, where terrorism should not have place but Some Scholars and experts say that the democracy is facilitator or instigator for terrorism because of its openness.
- ❑ Psychological sources of terrorism: The process of the emergence and formation of terrorism is to a large extent related to psychological factors, and it is strictly coupled with issues of hatred, prejudices, familiarity and alienation, intolerance, injustice, retaliation, trauma, and so on.
- ❑ Terrorism due to Alienation or Discrimination: Many groups of peoples came from their home land to other countries for employment or education and ultimately settled there. Many times, they face discrimination from the original citizens of the countries where they shifted. These groups may become jaded towards the society and feel excluded. Due to sentiments of discrimination and isolation, these groups become more conservative and start terrorist acts against the original citizens and government.
- ❑ The four major roles of anti-terrorist agencies are:
 - Intelligence gathering
 - Training and operations
 - Investigations
 - Prosecution

Drawbacks of Intelligence Infrastructure in dealing with terrorism

- ❑ India has a multitude of intelligence agencies. These various departments are supposed to coordinate and cooperate with one another in the sharing of intelligence. However, coordination on the ground is not up to the mark. Experts also opine that there is competition among intelligence agencies which prevents information sharing. Examples: Mumbai attacks brought these failures to the fore.
- ❑ Lack of Resources - A crucial weakness that most intelligence agencies suffer from is the lack of resources. They most often fall short of trained officers and finances. The case of NIA is an example. The elite agency was created in response to the Mumbai attacks and is modelled on the Federal Bureau of Investigation's counter-terrorism wing. Headquartered in Delhi and having 6 branch offices, the agency is facing as much as 30% manpower shortage on its sanctioned strength of a little over 800 people.
- ❑ Non-Unified Institutional Structure - There are a multitude of investigative and law enforcement agencies at the center and in the states which are responsible for law and order. The Central and state agencies coordinate through joint committees and task forces. But these are very slow and because of mistrust competition over resources, or simply incompetence, are unable to integrate efforts in any difficult situation.

- ❑ Lack of adequate Legal Provisions - Moreover, there are legal provisions that are unaddressed still. India till date does not have a comprehensive law to fight terrorism. There is a cobweb of acts dealing with issues of internal security which include the National Security Act of 1980, the Code of Criminal Procedures of 1973, the Arms Act of 1959, the Explosive Substances Act and 1908, the Armed Forces (Jammu and Kashmir) Special Powers Act of 1990, the Armed Forces Special Powers Act of 1958 and the Religious Institution (Prevention of Misuse) Act of 1988.

Institutional Framework to Tackle Terrorism

- ❑ Intelligence: IB (Intelligence Bureau), RAW (Research and Analysis Wing) and MAC (Multi Agency Centre) are involved in gathering intelligence. Multi Agency Centers collate intelligence information from different sources and disseminate them from different states as well as centres as such.
- ❑ Counter Terror operations: Counter Terror Operations are carried out by NSG (National Security Guard) and local police. The local police act on the ground, and are many a times the 1st responders. Other agencies like the Army and the special elite forces are also involved as and when required in aid of the civilian force.
- ❑ Center State Relations and Counter Terrorism: From the legal angle, law and order and police are state subjects. But Article 355 enjoins upon the Union duty to protect the state and entry 2-A of Union List gives power to the Union to deploy its forces in aid of civil power of the state. These clear the issues regarding federal arrangements and issues thereof.
- ❑ National Investigation Agency (NIA): The National Investigation Agency (NIA) is a federal agency established by the Indian Government to combat terror in India. NIA has concurrent jurisdiction which empowers the Centre to probe terror attacks in any part of the country, covering offences, including challenges to the country's sovereignty and integrity-, bomb blasts, hijacking of aircraft and ships, and attacks on nuclear installations.
- ❑ NATGRID: The National Intelligence Grid or NATGRID is an integrated intelligence grid that will link the databases of several departments and ministries of the Government of India so as to collect comprehensive patterns of intelligence that can be readily accessed by intelligence agencies. It is a counter terrorism measure that collects and collates a host of information from government databases including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel.
- ❑ Revamping of Multi Agency Centre (MAC): MAC is a multi-agency centre to counter terrorism whose mandate is to share terrorism related intelligence inputs on a day-to-day basis. Multi Agency Centre (MAC) was created in Delhi and Subsidiary Multi Agency Centres (SMACs) in various states comprising representatives from various security agencies for streamlining intelligence efforts after the Kargil war. But it was revamped after 26/11.
- ❑ Coastal Security Scheme Revamped: The issue of maritime security and the lack of it surfaced, and gained much attention after the Mumbai attacks. To strengthen the coastal security of the country, a series of measures have been taken to review, upgrade, and strengthen the coastal security of the country
- ❑ Call for adoption of Comprehensive Convention on International Terrorism (CCIT): it is a proposed treaty which provides a comprehensive global legal framework against terrorism.
- ❑ Cooperation with USA: In 2011, US-India Homeland Security Dialogue was created, which was the first comprehensive bilateral dialogue on homeland security issues between the two countries. The US Department of State Anti-Terrorism Assistance (ATA) programme also provided training to over 250 Indian law enforcement officers. .
- ❑ Part of Global Network of Cities on Terror Fight: Mumbai has now become part of this network formed at UN that will exchange techniques and develop infrastructure to combat extremism and strengthen their cyber security system.

Legal Framework to Deal with Terrorism

- ❑ The first special act to deal with terrorism was the Terrorist and Disruptive Activities (Prevention) Act or TADA. It came into force after Indira Gandhi's assassination. But following the allegations of its misuse, it was allowed to lapse in 1995, and another special act called the Prevention of Terrorism Act (PC) I A) was enacted in 2002, in the aftermath of the December-2001 attack on the Parliament. POTA was also repealed in 2004. After the 26/11 Mumbai Terrorist attack the Unlawful Activities (Prevention) Act (UAPA) Amendment Act came to force in December 2008, which was further amended in 2012.

Various Global Actions for countering Terrorism

- ❑ United Nations oversees various conventions that target different aspects of terrorism, including terrorist financing, hijacking, acquiring weapons of mass destruction, and hostage taking, to name a few.
- ❑ UN launched a new framework "UN Global Counter- Terrorism Coordination Compact".
- ❑ UN General Assembly unanimously adopted in 2006 the Global Counterterrorism Strategy (GCT).
- ❑ Counterterrorism Implementation Task Force (CTITF)—a partnership of bodies created by UN in 2005, which now includes more than thirty UN entities plus INTERPOL, to streamline and coordinate counterterrorism efforts within the UN.
- ❑ UNSC established the Counter terrorism Committee (CTC)
- ❑ Terrorist Travel Initiative was launched under auspices of Global Counterterrorism Forum (GCTF). It will bring together national and local governments, law enforcement and border screening practitioners, and international organizations to share expertise on how to develop and implement effective counterterrorism watch listing and screening tools.
- ❑ Financial Action Task Force (FATF) and the Group of Eight (G8) Counter terrorism Action Group (CTAG)
- ❑ European Union's the EU judicial cooperation unit, EUROJUST and the EU's police force, EUROPOL.

Way forward

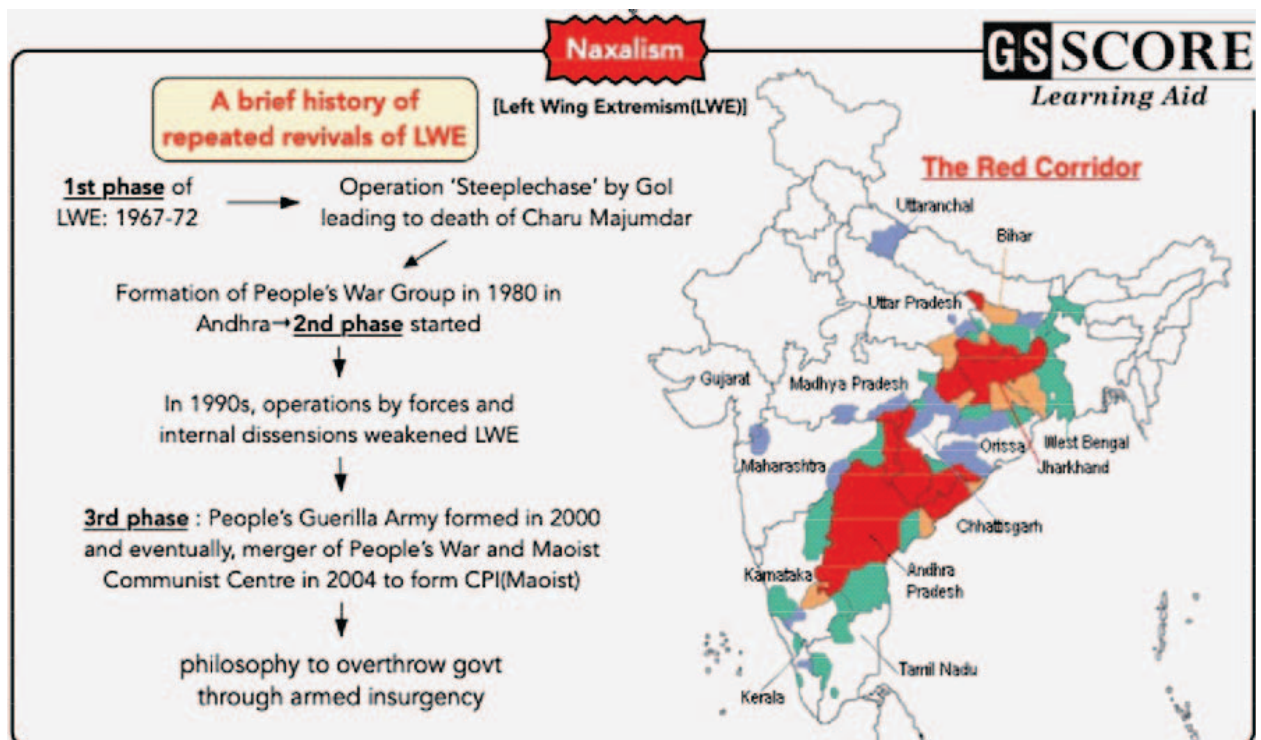
- ❑ Dealing with the menace of terrorism would require a comprehensive strategy in which different stakeholders, i.e., the Government, political parties, security agencies, civil society, and media would have an important role to play.
- ❑ Political: A strong political consensus should be built in the country which says that national interest is supreme and, in national interest, many issues are non-negotiable. They should not be discussed in media or any other public platform. They should not be decided on vote-bank politics or party lines.
- ❑ Legal: We need to have very stringent laws against terrorism, and fast track courts which can deliver judgment within 3-4 months.
- ❑ Police: Strengthening the state police, enhancing their training capabilities and providing them with modern equipment for surveillance, investigation and operations is the need of the hour. We need to have modern scientific forensic laboratories.
- ❑ Media: The role of the media is also very crucial in the fight against terrorism.
- ❑ Deterring terror would require focussed resource-rich responses in dismantling the various links in the terror chain like finances, weapons networks, actors etc. Special Forces with focused expertise on dismantling terror finances, the networks, and the cells are a must. Since any act of terror is a process that starts much ahead of the actual strike, key intelligence on the process can only be tracked by personnel trained in counter-terrorism, which would avert attacks.
- ❑ Vulnerable communities should be identified and the state's presence increased to deter them from falling prey to terror narratives of emancipation. This has to be done in a sensitive manner. State

presence should first focus on providing good governance in terms of health, education, employment, etc, and law enforcement done in a way that is sensitive to local culture.

- ❑ The state's counter-terror mechanism must envision the creation of Special Forces meant specifically for the purpose of averting terror networks in India. These Special Forces must be established in vulnerable states like Delhi, Maharashtra, Gujarat, Rajasthan, Manipur and Assam.
- ❑ The state's land and coastal border security must be strengthened given the fact that terror attacks have been conducted and planned in the neighbouring states.
- ❑ The state must also be well equipped to deal with the rising challenge of cyber-terrorism. Cyber specialization should be made a part of the counter-terror mechanism towards addressing hacking issues, tracing terror links in the virtual world, locating the computers, and countries where this transnational nature of terrorism originates, etc.

NAXALISM

Phase of Naxalism



Stated Purpose of the Naxal Movement

- ❑ The Naxalites state their main political purpose as establishing an alternative state structure in India by creating a "red corridor" (the Red Corridor is the region in the eastern, central and the southern parts of India that experience considerable Naxalite-Maoist insurgency) in Naxalite-affected states, stretching from the border of Nepal to central India to Karnataka in the south through violent struggle.
- ❑ To achieve this political objective, which requires local support, Naxalite rebel leaders take up causes like protecting people's rights of Jal, Jangal and Jamin (water, forest, and land) and providing justice through their committees like the Sangam and Jan Adalat (people's court).
- ❑ Local support is crucial for the Naxalites for cadre recruitment, intelligence, logistics, and territorial

control. The Naxalite movement engages in guerrilla warfare against the Indian security forces, as propounded by Mao Tse Tung.

- ❑ The ultimate objective is to attain political power by violent means and establish what they envisage as “The India People’s Democratic Federal Republic’. The naxalites predominantly attack the police and their establishments. They also attack certain types of infrastructure, like rail and road transport and power transmission, and also forcibly oppose execution of development works, like critical road construction.
- ❑ Naxalite activity is also manifesting itself through various civil society and front organizations on issues such as SEZ policy, land reforms, land acquisition, displacement, etc., with the objective of expanding their mass base and acquiring support of some intellectual elite.
- ❑ While impending development works and challenging State authority, the naxalites simultaneously try to derive benefit from the overall under development and sub-normal functioning of field institution like police stations, tehsils, development blocks, schools, primary health centres and anganwadi centres, which administer and provide services at ground level and also reflect the State Presence and writ.

Factors responsible for the growth of Naxalism:

- ❑ The Naxalite movement came into being as a result of prevailing social and economic issues. In fact, while conducting an enquiry into the uprising, the West Bengal State Secretariat of the CPI (M) stated, “Behind the peasant unrest in Naxalbari lies a deep social malady – malafide transfers, evictions and other anti-people actions of tea gardeners and jotedars.” These issues were longstanding and there was no dearth of reform legislation. But the spirit of the law remained confined to paper and the people were left to languish. Therefore, it recognized that the causes were in essence, socio-economic.
- ❑ After independence the Indian government started the protracted and difficult process of abolishing the Zamindari system, to eliminate the role of intermediaries. By the end of the 1950s, the process was completed on paper. This meant that 20 million erstwhile tenants were now landowners. One rough estimate says that area under tenancy declined from 42% to around 20% by early 1960s. However, to a large extent this was caused due to eviction of tenants by landlords and not by actual reform in the system.
- ❑ The next part of land reform was tenancy reform. Its objectives were to guarantee security of tenure to tenants, to ensure fair rent rates and to gain rights of ownership of land he/she cultivated, subject to some restrictions at well below market rates.
- ❑ In west Bengal, two major acts for land reform were passed in the 1950s aimed to eliminate intermediaries (zamindars and jotedars) and bring fixed rent tenants into a direct relationship with the state. It gave the state powers to inquire into land transfers and cancel the transfer if it was not bona fide. Abolition of intermediaries was generally successful. However numerous loopholes and poor implementation meant that the landlords were able to retain control over large tracks of land. It did not protect the rights of Bargadars (sharecroppers), who were the most deprived section of society.
- ❑ From 1947 to 1969, as part of land reform implementation in west Bengal, only 300,000 acres of above-ceiling land was redistributed, a little less than 3% of the cropped land in the state. The 1961 census estimated that 82 percent of the tenancies in the country were insecure. Bargadars received no protection until 1970, when the government, woken from stupor by the Naxalbari uprising amended the west Bengal land Reforms Act to cover them also. The legislations themselves were not strong enough and implementation was extremely ineffective.
- ❑ **Mismanagement of Forests:** It is one of the main reasons for the spread of Naxalism. It started with the British government. The monopolization of the forest started with the enactment of various forest laws. The integration with the wider world led to an influx of a new class like moneylenders. The administrative machinery became more exploitative and extortionate at functional level.

- ❑ **Tribal policies not implemented well:** Even during the post Independence era, the government was not able to stop the process of the tribal alienation and their displacement caused by large projects. Even the issues of food security were not fully sorted out. Consequently, Naxalism made inroads in Orissa and other states.
- ❑ **The Growing inter and intra regional disparities:** Naxalism attract people who have poor livelihood like fishermen, farmers, daily labourers and bamboo cutters. The government policies have failed to stem the growing inter and intra regional disparities. The poor people think that Naxalism can provide solutions to their problems.
- ❑ **Absence of proper Industrialisation and lack of land reforms:** The half-hearted implementation of land reforms by the government has yielded negative results. The agrarian set up has not been defined in the absence of proper implementation of survey and settlement. This further damaged the agriculture production and the rural economy. Absence of proper industrialization has failed to generate employment for rural people leading to dissatisfaction with the government. It is also one of the causes behind Naxalism.
- ❑ **Geographical Terrain:** Naxalism thrives in areas covered with forests. It helps them fight against the police and the army by waging Guerrilla warfare.
- ❑ Hence, Naxalism was the brain-child of exploitative relation of landlords and peasants, but today it has become one of the biggest security problem for India's future

Why naxalism is biggest threat to internal security?

- ❑ Former Prime Minister Manmohan Singh said "Naxalism is the biggest internal security challenge and it is imperative to control Left-wing extremism for the country's growth".
- ❑ The Naxalite threat is indeed the biggest security problem for India's future as its effects are multi-layered. The Maoist movement highlights India's interior weaknesses, which makes India also vulnerable to external threats too. As part of globalisation, threats such as the Naxalite movement can no longer be viewed as simply internal, as it also affects external security.
- ❑ The Naxals' potential for violence has increased substantially with their acquisition of sophisticated weapons and expertise in the use of improvised explosive devices (IEDs). They are said to be in possession of at least 6,500 regular weapons including AK 47 rifles and SLRs. They have built this arsenal essentially by looting weapons from police/landlords, purchasing them from smugglers, acquiring from insurgent groups like the NSCN (IM) and ULFA and also obtaining some weapons from Nepal.
- ❑ The Naxalite groups' nexus with the other extremist organizations has added to the complexity of the problem. There are indications that the PWG cadres received training in the handling of weapons and IEDs from some ex-LTTE cadres. They have also some understanding with the National Socialist Council of Nagaland (I-M) to support each others' cause. Some batches of CPML-Party Unity also appear to have received arms training under the guidance of United Liberation Front of Assam. The Communist Party of India (Maoist) has close fraternal relations with the Communist Party of Nepal (Maoist) also.
- ❑ Another reason why the Naxalites are the biggest threat to security is because of the way the issue affects India's economic development. This is apparent in several ways. For example, the more the Maoists concentrate on the poor and marginalised regions of India, the more economic development (which is imperative to improving those regions' conditions) will be hampered. Furthermore, the Naxalite rebels are no longer just focussing on remote jungles but on urban centres. Maoist leader Kishenji even declared that the group aims to establish an armed movement in Calcutta by 2011. Internal order and stability are necessary for a nation's economic development.
- ❑ For India to continue being able to withstand outside security threats, it must build up its infrastructure, its defence and its people. In terms of lifting its citizens out of poverty, India has a long way to go, and

continued economic growth is integral to India's development as a strong global player. The Naxalite activities are using up scarce resources on defence and internal security when it should be spent on areas such as social development.

Urban Naxals:

The term Urban Naxals is not clearly defined. The origin of the word can be traced to the book and a few essays by film-maker and social media opinion-maker Vivek Agnihotri's book, Urban Naxals: The Making of Buddha in a Traffic Jam.

The phrase of Urban Naxals is loosely attributed to the people with naxalite bent of mind residing in urban areas and working as activists, supporters, and protectors of the ideology while the active Naxals battle it out in the jungles and vast swathes of Maoist-dominated areas.

Maoists have an old strategy of looking into urban centres for leadership, organise masses, build a united front and engage in military tasks such as providing personnel, material and infrastructure. This was highlighted even in their 2004 Communist Party of India (Maoist) document titled "Urban Perspective" which elaborates on this strategy with one of the most important focus areas being on gaining leadership from urban areas.

How Naxal insurgency continues to survive?

- ❑ One the primary reasons for the survival of the naxal is the local support, which makes difficult for the security forces to get accurate information about the insurgents. Besides, the naxal get information about the movement of the forces through villagers and some government officials. Here are some the reasons:
- ❑ Good knowledge about topography: Insurgents have thorough knowledge about the area they are in, whether it is hill, forest etc.
- ❑ Supply of weapons: Naxal procure arms in several ways including raids in a police station or by buying small guns from local people.
- ❑ Using tribal as human shield: Despite getting intelligence inputs, security forces are hindered by the presence of tribal men as human shields.
- ❑ Lack of quality roads: Lack of good quality proves to be the major stumbling block for security forces for their movements.

Government's Approach to deal with Left Wing Extremism (LWE)

- ❑ 'Police' and 'Public order' being State subjects, action with respect to maintenance of law and order lies primarily in the domain of the concerned State Governments.
- ❑ The underlying philosophy is to enhance the capacity of State Governments to tackle the LWE menace in a concerted manner.
- ❑ The policy of the Government of India is to effectively deal with the LWE insurgency primarily by augmenting the capacity of the State Governments both in areas of security and development. Accordingly, the Government of India is implementing schemes for improving the security environment. Simultaneously, focused attention is also being paid to development and governance issues particularly at the cutting edge level.
- ❑ The Government of India is providing funds to the States under various Central Schemes for improving the basic infrastructure like road & rail connectivity, mobile connectivity, educational & health initiatives, electrification etc.

- ❑ Government of India launched SAMADHAN doctrine 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
- ❑ Forest Rights Act: This Act was enacted primarily to safeguard the rights of the tribals who have been living in forests for generations and to mitigate the injustice by earlier forest Acts (e.g., Indian Forest Act 1927, Wild Life Protection Act 1972, Forest Conservation Act, 1980).
- ❑ Education initiatives: The opening of residential schools has been quite effective in retaining children in schools. The coordination with Ashram Shalas and other SC/ST department schools by giving free text books, the mid day meal, teacher training school maintenance grant and teacher grant for teaching aids has been helped. Multi-Lingual Education in early grades in tribal districts of Odisha, Andhra Pradesh and Chhattisgarh is another step that can improve learning comprehension and retention of children in schools.
- ❑ Integrated Action Plan (IAP): The objective of the scheme was to build public infrastructure and provision some basic services like school, anganwadi centres, primary health centres, drinking water supply, roads, etc.
- ❑ Panchayat Extension to Scheduled Areas Act (PESA): The key objective of the Act was to empower the local Gram Sabha for efficient management of natural and community resources; conservation and protection of traditional customs and rituals; and management of non-timber forest products.
- ❑ Balbandhu Programme of National Commission for Protection of Child Rights: An innovative Balbandhu scheme initiated by the National Commission for Protection of Child Rights (NCPCR) in strife torn areas two years back has started making an impact too.
- ❑ Ban on the CPI (Maoist): The CPI (Maoist) which is the major Left Wing Extremist organization and responsible for most incidents of violence/casualties, has been included in the Schedule of Terrorist Organisations, along with all its formations and front organizations under the existing Unlawful Activities (Prevention) Act 1967 since 22nd June 2009.
- ❑ Strengthening the Intelligence Mechanism: This includes intelligence sharing through Multi Agency Centre (MAC) at the Central level and through State Multi Agency Centre (SMAC) at the State level on 24x7 basis.
- ❑ Better Inter-State Coordination: The Government of India has taken a number of steps to improve Inter- State coordination through periodic Inter-State meetings and also facilitating interactions between the bordering districts of LWE affected States.
- ❑ Tackling the Problem of Improvised Explosive Devices (IEDs): Majority of Security Forces casualties are being caused by IEDs. The MHA continues to support extensive counter-IED capacity building efforts of CAPFs and State Police Forces.
- ❑ The Scheduled Tribes and Other Traditional Forest Dwellers (Recognition of Rights) Act, 2006: The Government has enacted the Act to recognize and vest the forest rights and occupation on the forestland to forest dwelling Scheduled Tribes and other traditional forest dwellers, who have been residing in such forests for generations, but whose rights could not be recorded.

Major Sub – Schemes under Scheme Modernization of Police Forces for 2017-20

- ❑ **Security Related Expenditure (SRE) Scheme:** It aims at strengthening the capacity of the LWE affected States to fight against the LWE problem in an effective manner.
- ❑ Special Central Assistance (SCA) for 35 most LWE affected districts which have the main objective of filling the critical gaps in Public Infrastructure and Services, which are of emergent nature.
- ❑ Special Infrastructure Scheme (SIS) including construction of 250 Fortified Police Stations in LWE affected states. The Scheme aims at capacity building of states by strengthening the security apparatus of the States.
- ❑ **Assistance to Central Agencies for LWE management Scheme:** Assistance is provided to Central Agencies like CAPFs, Commando Battalions for Resolute Action (CoBRA), Indian Air Force for anti LWE Operations, where the States have constraints.
- ❑ Civic Action Programme (CAP) is being implemented since 2010-11 to bridge the gaps between Security Forces and local people through personal interaction and bring the human face of SFs before the local population. Under the Scheme, funds are released to the CAPFs, deployed in LWE affected areas, for conducting various civic activities in welfare of the local people.
- ❑ **Media Plan Scheme:** to counter the Maoist propaganda of misguiding and luring the innocent tribals/ local population by their so called poor-friendly revolution.
- ❑ **Reserve Battalion (SIRB):** The Left Wing Extremism affected states have been sanctioned India Reserve (IR) battalions mainly to strengthen their security apparatus at their own level and also to enable the states to provide gainful employment to youth, particularly in the LWE affected areas.
- ❑ **Modernization of Police Force (MPF):** The focus of the scheme is to strengthen police infrastructure at cutting edge level by construction of secure police stations, training centres, police housing (residential), equipping the police stations with the required mobility, modern weaponry, communication equipment and forensic set-up etc.

Infrastructure development initiatives

- ❑ Road Requirement Plan-I (RRP-I) is being implemented by the Ministry of Road Transport & Highways, since 2009 for improving road connectivity in 34 LWE affected districts of 8 States. It envisages construction of 5,422 km road lengths and 08 critical bridges in LWE affected States.
- ❑ Road Connectivity Project for LWE affected areas (RRP-II): It was approved in 2016 for further improving road connectivity in 44 districts of 9 LWE affected States. Ministry of Rural Development (MoRD) is the nodal Ministry for this project.
- ❑ LWE Mobile Tower Project to improve mobile connectivity in the LWE areas.
- ❑ Approval of Projects under USOF - Union cabinet has approved the Universal Service Obligation Fund (USOF) supported scheme to provide mobile services in 96 districts of LWE-affected states to help not only in communication with the security personnel, but also, for the residents of these areas.
- ❑ The National Technical Research Organization (NTRO) is assisting the Security Forces in anti-Naxal operations by providing Unmanned Aerial Vehicles (UAVs).

Skill Development related Schemes

- ❑ ROSHNI is a special initiative under, Pandit Deen Dayal Upadhyaya Grameen Kaushalya Yojana, which envisages training and placement of rural poor youth from 27 LWE affected districts.
- ❑ Skill Development in 34 Districts affected by Left Wing Extremism” under implementation from 2011-12 aims to establish ITIs and Skill Development Centres in LWE affected districts.
- ❑ Surrender and rehabilitation policies: State Governments have their own policy, while the Central

Government supplements the efforts of the State Governments through the Security Related Expenditure (SRE) Scheme for LWE affected States. Additional incentives are given for surrendering with weapons/ammunition. The surrenderees are also imparted vocational training with a monthly stipend for a maximum period of 36 months.

Institutional measures

- ❑ Black Panther combat force - A specialised anti-Naxal combat force for Chhattisgarh on the lines of Greyhounds unit in Telangana and Andhra Pradesh.
- ❑ Bastariya Battalion – A newly formed battalion of CRPF, with more than 534 tribal youth from four highly naxal infested districts of Chhattisgarh along with adequate female representation in sync with the Government's policy of 33% reservation for women making it the first composite battalion in any of paramilitary forces.

Improvement in the Left Wing Extremism (LWE) scenario:

- ❑ Over the last decade or so, there has been consistent decline both in the violence figure and its geographical spread.
- ❑ The incidents of LWE violence has come down by 70% from a all time high of 2258 in 2009 to 665 in 2020.
- ❑ The resultant deaths of has also come down by 82% from all time high of 1005 in 2010 to 183 in 2020.
- ❑ The area under Maoist's influence was also constricted with the geographical spread shrunk from 96 in 2010 to just 53 districts in 2020. These miscreants have been pushed to a few pockets with only 25 districts accounting for 85% of the LWE violence in the country.

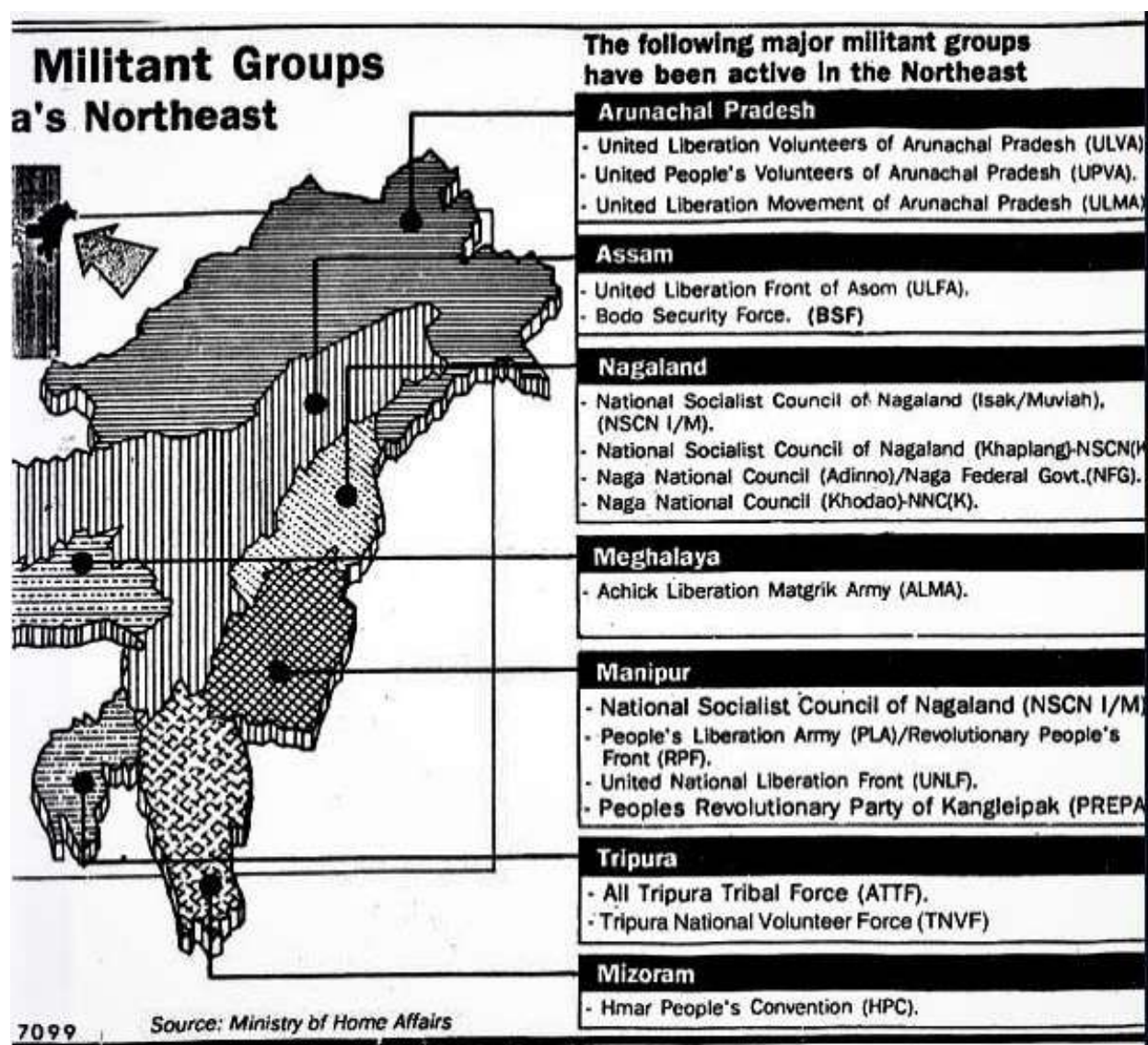
Suggestion:

- ❑ Good governance: The presence of Naxals in the country also reveals the loopholes in the law and order of the country which has failed to curb the menace. Central government needs to implement a coherent national strategy to end Naxalism.
- ❑ Dialogue: Dialogues between the Naxal leaders, and the government officials can be a way work out a solution.
- ❑ Generate more employment and increase wages: Insecure livelihood and unemployment in the areas have left the people with no option but to join the Naxals.
- ❑ Rehabilitation and resettlement: Mining grounds, irrigation areas, industries, etc., in the area without any provision for the resettlement of the displaced people has only added to the woes of the poor. There needs to be more emphasis on rehabilitation of these affected population
- ❑ Prevent environmental degradation: Environmental degradation in the form of destruction of land and water resources due to mining and industrial activates. The locals are left with disrupted lives and adversely affecting tourism.
- ❑ Stop the political marginalization of weaker sections: Weaker sections of the society, the schedule castes and schedule tribes still face discrimination from the upper class which needs to be minimized.
- ❑ Remove disparity: Economic disparity and the growing distance between rich and the poor is one of the main problems that has contributed to the growth of Naxalism
- ❑ Modernize law enforcement agencies: Central government must inroads into these disturbed states with their agencies well-equipped with modern artillery and assist the usually poorly-equipped agencies of the state.

Insurgency in North-East

Issues & Conflicts

- For more than half-a-century, the North East has seen an unending cycle of violent conflicts dominated by insurgencies with demands ranging from outright sovereignty to greater political autonomy. Indirectly, insurgent movements have spawned a variety of related conflicts. Insurgency has taken a toll of thousands of lives, both of security forces and citizens.
- Conflicts in the region range from insurgency for secession to insurgency for autonomy and from 'sponsored terrorism' to ethnic clashes, to conflicts generated as a result of continuous inflow of migrants from across the borders as well as from other States.



Reasons for Insurgency in the Northeast

- After partition, the Northeastern Areas (Re-organisation) Act, 1971 created three states – Manipur, Tripura and Meghalaya and two Union Territories, Mizoram and Arunachal Pradesh effective from January 21, 1972. The two Union Territories became states in 1987. All the states in the Northeast

are in the grip of insurgency or have been through insurgency in the past. The reasons for these are similar and have been enumerated below:

- The roots of insurgency in the area go back to pre-independence days. The tribes were not brought under a strict political control and rigid regulations. The British tribal policy and Christian education are believed to have queered the pitch for Independent India.
- Setting up of reserved forests by British led to the loss of tribal control over natural resources.
- Migration of people from the plains posing economic, cultural and political threat to the tribals.
- Lack of good governance and transparency,
- Faulty nation-building strategies (economic deprivation).
- Inappropriate development.
- Large-scale unemployment.
- Hostile neighbours extending moral and material support.
- Lack of good leadership and popular support.
- Not anti-India but anti-establishment.
- Money for development never reached the target but was diverted to insurgents by politicians to buy security. There was no shortage of recruits as unemployed educated youth were available to join them.
- Tensions between these states and the central government.
- Tensions between tribal people, who are natives of these states, and migrant peoples from other parts of India.
- Geographical reasons – not well connected with present Indian mainland.
- Developmental reasons – Poorly developed due to lack of fund from Center/States.
- Military reasons – AFSPA (Armed Forces Special Power Act).

Reasons for cross border insurgency

- ❑ Safe Havens: The shelter and support that the Indian insurgent groups receive from across the border have been one of the most important factors which have helped them in sustaining their rebellion.
- ❑ Economic support: The Golden Triangle (comprising Myanmar, Laos and Thailand) has provided an economic boom for the insurgent groups to sustain themselves.
- ❑ Availability of weapons: Easy availability of small arms in neighboring countries like Bangladesh and Myanmar has been another factor behind the sustenance of insurgency in the region.
- ❑ Ethnic affinity: Many ethnic groups in the region, especially in the areas bordering the international boundaries, have more in common with the population living across the boundary than with their own nationals.

Border issues in North east:

- ❑ Terrain of Border: Difficult terrain along border with different countries in north east make means of transportation and communication difficult and as a result, the border area remains sparsely populated with depressed economic development.
- ❑ High mountains, deep river channels together with lush forest characterize the borderland with Myanmar.
- ❑ Inaccessible forested areas along the Assam– Bhutan border continue to serve as temporary bases and safe havens for the insurgent groups.

- ❑ River line borders in Bangladesh tend to change course periodically, leading to a host of disputes associated with the difficulties in establishing ownership of the newly created territories.
- ❑ Boundary issue: Even though the international boundary between countries like India and Myanmar had been formally delimited and demarcated following the boundary agreement in March, 1967, the boundary has not crystallised on the ground as lines separating two sovereign countries.
- ❑ Free movement regime: India-Myanmar border has a unique arrangement in place called the Free Movement Regime (FMR). The FMR permits the tribes residing along the border to travel 16-km across the boundary without visa restrictions.

Challenges in handling insurgency

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

Improved security situation in the North Eastern States

- ❑ The security situation in the northeastern states has significantly improved since 2014, and the year 2020 saw the fewest insurgency incidents and casualties among citizens and security forces in the previous 20 years, according to the Ministry of Home Affairs' annual report.
- ❑ "Insurgency events in 2020 have decreased by 80% as compared to 2014. In a similar vein, civilian deaths have decreased by 98% while security forces injuries have decreased by 75% over this time.
- ❑ The number of insurgency occurrences (223 in 2019 and 162 in 2020) and civilian and security force casualties decreased by around 27% and 72%, respectively, in the year 2020.
- ❑ In 2020, the counterinsurgency operations in the area resulted in the neutralisation of 21 insurgents, the arrest of 646 insurgents, and the recovery of 305 weapons.
- ❑ Up to 2,644 cadres of insurgent groups from the northeastern states gave up their weapons and assented to society in 2020.
- ❑ The security situation in other states of the region has significantly improved, while Mizoram, Sikkim, and Tripura remained largely quiet.
- ❑ In comparison to 2019, insurgency-related violence decreased by 42% in Arunachal Pradesh, 12% in Assam, 23% in Manipur, and 45% in Nagaland in 2020.

❑ Bodo Accord

- ❑ The government of India has signed three agreements with Bodo tribes so far for 27 years.
- ❑ The All Bodo Students Union (ABSU) and the Government of India have signed the first accord in 1993. This agreement resulted to the creation of a Bodoland Autonomous Council with some political powers.
- ❑ The second Bodo accord was signed in 2003 between Government of India and extremist group Bodo Liberation Tigers (BLT).

- The second agreement resulted to the formation of Bodoland Territorial Council (BTC) with four districts – Udalguri, Chirang, Baska and Kokrajhar. These areas are commonly called Bodoland Territorial Area District (BTAD).
- The 3rd Bodo Peace Accord as tripartite agreement between the Centre, Assam Government and the banned Assam-based insurgent group National Democratic Front of Bodoland (NDFB) was signed on 27th January 2020, for bringing a lasting peace in Bodo-dominated areas in Assam.

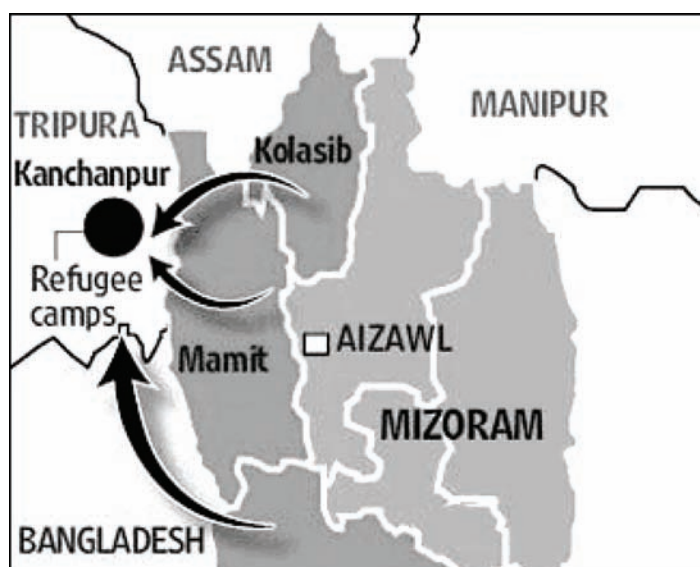
Highlights of the 3rd Bodo Peace Accord:

- Villages dominated by Bodos presently outside Bodo Territorial Area District (BTAD) would be included and those with non Bodo population would be excluded.
- Bodos living in hills would be conferred Scheduled Hill Tribe status.
- Bodo with Devnagri script would be associate official language for entire Assam.
- BTAD would now be called Bodoland Territorial Region and it will have more executive, administrative, legislative and financial powers.
- Over 1500 armed cadres will abjure violence and join mainstream.
- A Special Development Package of Rs. 1500 crores over three years is provided.

Concerns remain

- Concerns of the non-Bodos: Critics have alleged that accord has ignored the interests of the other ethnic communities in the area. Concerns of non-Bodo people, mainly Bengali-speaking Muslims, Adivasis, and migrants inhabiting these districts, who were attacked and killed in large numbers in all these years, must be addressed.
- Implementational issues: Biggest challenge before all the stakeholders, including the government, would be to make it sustainable by enforcing commitments given in the new peaceaccord.
- Possibility of a chain reaction: The accord could trigger similar demands in other parts of Assam, such as Karbi Anglong, Dima Hasao and Cachar, which also have homelands of non-Ahom ethnicities.
- Moreover, it could also affect the ongoing Naga peace process, leading Naga rebels to demand territorial and administrative autonomy in Naga homelands in Manipur, which will further trigger political and ethnic tension between the Nagas and the Meitei (the largest ethnic group in Manipur).

Repatriation of Bru Migrants from Tripura to Mizoram



- ❑ Due to ethnic violence in the western part of Mizoram in October 1997, a large number of minority Bru (Reang) families migrated to North Tripura in 1997-1998.
- ❑ In 2010, GoI began its efforts to permanently rehabilitate them as they constantly demanded to settle in Tripura. In 2018, GoI signed an agreement with the State Governments of Tripura and Mizoram in order to help the families and increase the aid substantially.
- ❑ On January 17, 2020, Government of India, Bru-Reang representatives, Government of Tripura and Mizoram signed an agreement in New Delhi to end the refugee crisis of Bru-Reang community.

Steps taken by Government to deal with the situation of insurgency

- ❑ The Law & Order is a State subject. However, the Central Government is supplementing efforts of the State Governments for curbing the illegal and unlawful activities of militant/insurgent groups of North Eastern States through various measures.
- ❑ These include deployment of Central Armed Police Forces, reimbursement of security related expenditure to the State Governments under SRE Scheme, central assistance to the State Governments for modernization of State Police Forces, sanction of India Reserve Battalions, banning the Unlawful Associations operating in NE Region under UAPA, declaring specific areas/ states as 'disturbed areas' for the purpose of AFSPA and issuing notifications for Unified Command Structure.
- ❑ The implementation of the agreed Ground Rules of insurgent outfits is periodically reviewed by Joint Monitoring Groups comprising representatives of the Government of India, State Governments, Security Forces and the outfits concerned.
- ❑ Central Government has deployed Central Armed Police Forces (CAPFs) to aid the State authorities for carrying out counter insurgency operations and providing security to vulnerable institutions and installations.
- ❑ The Government of India is assisting the State Governments for augmenting and upgrading their police forces to deal with insurgency /militancy.
- ❑ Recently, the Parliament passed the Citizenship (Amendment) Bill 2019. In accordance with this Act , an illegal migrant is prohibited from acquiring Indian citizenship. An illegal immigrant is a foreigner who either enters India illegally, i.e., without valid travel documents, like a visa and passport, or enters India legally, but stays beyond the time period permitted in their travel documents.
- ❑ Due to security reasons, certain areas have been declared as Protected Area/Restricted Areas where no foreigner can enter or stay without obtaining permit from the competent authorities
- ❑ Operation Sunrise: The armies of India and Myanmar carried out a coordinated operation called Operation Sunrise 2 in their respective border areas, targeting several militant groups operating in Manipur, Nagaland and Assam.

About Operation Sunrise 2 :

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

Suggestions to curb insurgency in North East India:

- ❑ Political solutions: Meeting the political aspirations of groups by giving them autonomy.
- ❑ Development of the region: Focus of the Ministry of DoNER and NEC should be on investment in mega-projects which will make big difference to the development of the region.

- ❑ Act East Policy: Greater awareness about the Act East Policy and its benefits to the North East should be generated among the policymakers and the intelligentsia of the region.
- ❑ Strengthening of Regional Forums: Regional groupings like SAARC, BIMSTEC, BCIM can help in enhancing economic and security cooperation with these countries which will lead to a better understanding of benefits of peace in North-East India.
- ❑ Joint Training and operations: Exercises like “Hand in hand” with China, “Operation Sampriti” between India and Bangladesh etc. can help to combat terrorism.
- ❑ Sensitization of people: The border community should be sensitised to participate in the nation building project through sustained community interaction programmes.

Kashmir Issue

Root causes behind the Kashmir unrest

- ❑ Economic Causes: Even while militancy was in decline and a free and fair electoral system in place since 2002, the governance deficit remained large. Economic growth in the state almost consistently lagged behind the national growth figures. Widespread unemployment and lack of new job avenues.
 - ❖ Disintegration of traditional handicrafts
 - ❖ Poor industrial setup
 - ❖ Declining tourism due to terror attacks
 - ❖ Loss of crops due to floods, cloudburst, etc.
 - ❖ Issues in rehabilitation of flood victims, etc.
- ❑ Social causes: Poor education and health system, allegations of penetration of radical Islam in the majorly Sufi Islam region, wounds of 1980's insurgency and indoctrination of youth by radical leaders has further contributed to their despair.
- ❑ An atmosphere of mistrust: Fear and mistrust are central to this conflict. Fear of people belonging to another religion having a different value system that threatens one's own, as well as fear concerning the loss of control or the loss of power.
- ❑ External factors: Pakistan incites the sentiments of Kashmiri people especially youth, carries on cross-border infiltration to spread the unrest and uses terrorism as a diplomatic tool to worsen the situation.
- ❑ A confrontation between two nationalisms

Abrogation of Article 370

- ❑ On 5th of August 2019, the President of India promulgated the Constitution (Application to Jammu and Kashmir) Order, 2019.
- ❑ The order effectively abrogates the special status accorded to Jammu and Kashmir under the provision of Article 370 - whereby provisions of the Constitution which were applicable to other states were not applicable to Jammu and Kashmir (J&K).
- ❑ In addition, the Jammu and Kashmir Reorganisation Act was passed by the parliament, enacting the division the state of Jammu and Kashmir into two union territories to be called Union Territory of Jammu and Kashmir and Union Territory of Ladakh.

Before	After
Special Status	No special status
Dual citizenship	Single citizenship
Separate flag	No separate flag
RTI not applicable	RTI applicable
Right to education is not applicable in J&K	Right to education is now applicable in J&K
Citizens from other parts of the country cannot buy property in J&K	Citizens from other parts of the country can buy property in J&K

Steps taken by the government after abrogation of Article 270

- The development of the many projects being carried out in the UT of Jammu and Kashmir under the Prime Minister's Development Package, including those in the fields of roads, power, health, education, tourism, agriculture, and skill development.
- As part of the Swachh Bharat Mission, J&K was deemed Open Defecation Free (ODF). The Saubhagya, Ujala, Ujjwala, and Indradhanush programmes, as well as other beneficiary-focused programmes, have all reached 100% saturation.
- Under the Pradhan Mantri Gram Sadak Yojna, the 17601 km of road building was finished by March 2022. Udhampur-Katra, Banihal-Quazigund, and Quazigund-Baramulla sections have all been opened in order to connect Kashmir with trains.
- Recently, 15 new medical schools, 2 new AIIMS, 2 State cancer institutes, 7 new medical colleges, and 15 new nursing colleges have all been opened or put into operation. The Indian Institute of Technology (IIT) Jammu and the Indian Institute of Management (IIM) Jammu are both currently open for business. There are currently 147 government engineering/degree colleges, up from 96 earlier.
- In the past two years, power projects with a 3000 MW capacity have been restarted, and construction is progressing according to plan. Between Srinagar and Sharjah, an international flight has started. The High Density Plantation Scheme for Apple has been expanded to include mango, litchi, cherry, walnut, and other trees. Kashmiri saffron has been given the Geographical Indication (GI) designation.
- The Jal Jeevan Mission has led to an increase in the number of household tap water connections. In two districts, Har Ghar Jal districts have been established (Srinagar and Ganderbal). All rural schools, anganwari centres, and healthcare institutions have tap water hookups.
- The Main Ravi Canal, the third stage of the Tral Lift Irrigation Scheme, and the Comprehensive Flood Management Plan of the River Jhelum & its Tributaries-Phase-I are three large irrigation projects that have been completed.
- The Jammu and Kashmiri government hired 29,806 workers in total for the public sector starting in 2019. Furthermore, it is anticipated that self-employment programmes have contributed to the creation of work for 5.2 lakh individuals.

Current security situation in J&K

- The Kashmir Valley is currently under the worst security danger from faceless militancy. attacks that are specifically directed at migrants and police officers. The alleged insurgent has no criminal history or past convictions.
- Social media propaganda has become more widespread thanks to the internet, agitating the young of Jammu and Kashmir. One of the most important steps in catching the criminal is to cross-check the suspect's identity against databases.

- ❑ The funerals of young insurgent leaders have made them famous people. People try to follow them and mimic them.
- ❑ Government figures show that since January 2019, there have been at least 690 insurgent killings in J&K. Data show that over the same time period, 149 security personnel and 57 J&K Police officers perished. According to police statistics, there are currently at least 129 active militants in the region.

Over ground workers (OGWs)

- ❑ Over ground workers (OGWs) are people who help militants, or terrorists, with logistical support, cash, shelter, and other infrastructure with which armed groups and insurgency movements such as Hizbul Mujaheddin, and Jaish-e-Muhammad in Jammu and Kashmir can operate.
- ❑ The role played by OGWs: Supporting the insurgent with food and logistics. Among young people, propaganda and radical narrative, new militant hiring, Hawala business. The anti-state rally is planned and funded by them, just like throwing stones. Inputs such as operational planning, intelligence data, safety routes, maps, and other elements are provided by them.
- ❑ Issues in handling OGWs: Random booking of youth for suspected OGW activity can completely eliminates an individual's chance to come back to society and thus provide opportunity to the terrorists for indoctrination.
- ❑ Government's operations towards OGWs can embed strong 'Us vs. them' narratives amongst the population and alienate them from the Indian polity. OGWs are also capable of carrying out small scale strikes while retaining the capability to mix rapidly with the population.

Steps taken in India to deal with OGWs:

- ❑ Armed forces conduct Operation All Out to destroy insurgent networks, their OGW, and senior militant commanders. Indian Army's Operation Sadbhavana (Goodwill) in J&K to address the desires of those impacted by terrorism.
- ❑ Mission Pehal wants to encourage young people to voice their complaints against the Indian government, army officers, etc. Scholarships for higher education and income-generating programmes like USTTAD, Udaan, and Nai Manzil.
- ❑ Opportunities for training and employment exist for young people under numerous programmes, including HIMAYAT and PMKVY. Other actions taken by law enforcement agencies include tracking the flow of money to terrorist organisations by the NIA, sharing intelligence information in real time, etc.
- ❑ Through a multi-agency effort, it is vital to collectively map OGWs, terrorists, and anti-national groups in order to design and plan tactics that are in keeping with the realities on the ground.

The Khalistan Movement

The Khalistan movement is a Sikh separatist movement, which seeks to create a separate country called Khalistān ("The Land of the Pure") in the Punjab region to serve as a homeland for Sikhs. The territorial definition of the proposed country Khalistan consists of both the Punjab, India along with Punjab, Pakistan and includes parts of Haryana, Himachal Pradesh, Jammu and Kashmir, and Rajasthan.

Steps taken by government

- ❑ Enacting legislative framework such as The Unlawful Activities (Prevention) Act, 1967; The National Security Act, 1980; The Terrorist and Disruptive Activities (Prevention) Act (TADA), 1985 and 1987; Prevention of Terrorism Act, 2002 (POTA)

- ❑ Cooperation with USA: In 2011, US-India Homeland Security Dialogue was created, which was the first comprehensive bilateral dialogue on homeland security issues between our two countries. The US Department of State Anti-Terrorism Assistance (ATA) programme also provided training to over 250 Indian law enforcement officers.
- ❑ Part of Global Network of Cities on Terror Fight: Mumbai has now become part of this network formed at UN Level that will exchange techniques and develop infrastructure to combat extremism and strengthen their cyber security system.

Suggestions:

- ❑ Intelligence Agencies- There is a need for cooperation among centre, state, and international intelligence agencies.
- ❑ Proper Surveillance- It is of critical importance to penetrate the networks and sleeper cells of the terrorist organizations to gain actionable intelligence.
- ❑ Technology to detect and alert for suspicious activity such as loitering by an individual or vehicle should be made use of.
- ❑ Security personnel should be sensitized to spotting and segregating suspicious objects that are left behind.
 - Police, must be effectively trained to deal with this new phenomenon of urban terror.
 - Every state should have a NSG-type of commando force to counter lethal terror strikes.
 - Rehearsals should be periodically undertaken for search-and-rescue operations after large-scale terrorist strikes and different contingencies should be simulated and practiced.

De-Radicalization in India

De-Radicalization has been defined as the process of changing an individual's belief system, rejecting the extremist ideology, and embracing mainstream values.

Root causes of radicalization:

- ❑ Communities struck by poverty, disease, illiteracy, bitter hopelessness
- ❑ Social inequality, marginalisation and exclusion
- ❑ Political oppression and the violation of basic rights
- ❑ Injustices, misery, starvation, drugs, exclusion, prejudices, despair for lack of perspectives

Measures taken

- ❑ Counselling of 'vulnerable and radicalized' youths as well as their families and propagating 'moderate' interpretations of Islam to counter the Islamic State (IS) ideology.
- ❑ Various measures like an 'extremist counseling hotline', set up recently by Austria, has reportedly drawn the interest of Indian authorities.
- ❑ The viability of the US' counter-radicalisation programmes focused on community outreach and the UK's Prevent and Channel programmes in the Indian context is being considered.

Further steps needed

- ❑ Recognition of problem: Instances of communal violence should not be taken lightly or dismissed as

incidents typical to a united but dysfunctional family. India already has a highly radicalised population divided along communal and caste lines

- ❑ Involve civil society: The role of civil society can prove crucial in fighting the growing threat of radicalisation. It can foster a sense of belonging and shared identity and reduce real and perceived isolation among members of vulnerable communities and bridge internal community divisions
- ❑ Community outreach: There is a need to empower the moderate voice among all communities in order to separate radicals from the general population through effective home-grown community outreach programmes.
- ❑ Choke funding: There is also the need to track down the channels for the funding of certain religious organisations that may be spreading the poison of radicalization.
- ❑ Prevent politicization of religion: At the administrative level, there is a need to check growing politicisation of religion across the political spectrum by stringent implementation of existing laws and strict compliance of the code of conduct during elections.
- ❑ Introduce religious studies as a secular academic discipline in our universities, so that the false religious indoctrination of foreign extremist groups through the Internet can be countered. Religious leaders can also be encouraged to counsel against radicalization.
- ❑ Using cyberspace: The importance of developing a strong counter-radicalisation presence in the cyber world cannot be understated, particularly in the country's regional languages in which ISIS and Al-Qaeda. Various steps have been taken by the states. Maharashtra has rolled out a deradicalisation programme for the minority community in February 2016.

Communal Violence

Communal violence involves people belonging to two different religious communities mobilised against each other and carrying the feelings of hostility, emotional fury, exploitation, social discrimination and social neglect. The high degree of cohesion in one community against another is built around tension and polarisation. The targets of attack are the members of the 'enemy' community. Generally, there is no leadership in communal riots which could effectively control and contain the riot situation. It could thus be said that communal violence is based mainly on hatred, enmity and revenge.

Factors Responsible for Communal Riots

- ❑ The following factors are responsible for communal riots.
 - Historical factors: The history of partition and the two-nation theory have generated a deep sense of communalism and lack of mutual trust among both the communities. It discouraged a harmonious association and peaceful co-existence.
 - Political factors: Divide and rule policy practiced by the British and subsequent vote-bank politics followed by Indian political parties after independence have added to the divide between the communities. Lack of liberal, progressive and modern attitude in both communities has weakened the cause of communal harmony.
 - Educational factors: There is a lack of modern education among a large section of the Indian society. A majority of Indians failed to adopt a scientific and technological approach, hence are reluctant to adopt liberal, progressive values.
 - Socio-economic factors: Due to their educational backwardness, the Muslims have not been represented sufficiently in public services, industry and trade, etc. Their economic status is very low. This causes the feeling of relative deprivation and such feelings contain the seeds of communalism.

- Psychological factors: Psychological factors play an important role in the development of communalism. Both communities have perceived grudges against each other. There is a sort of fear psychosis amongst Muslims. These lead to communal ill-feelings.
- Identity crisis or identity factors: There is a feeling that Muslims are reluctant to join the national mainstream. Most of them do not enthusiastically participate in secular nationalistic politics and insist on maintaining their separate identity.
- Cultural factors: Orthodox members of both communities feel that they have a distinct entity with their own cultural pattern, personal laws and thought processes. There are strong elements of conservatism and fundamentalism among both the communities.
- The ISI factor: It is widely believed that the ISI is directly encouraging and promoting communalism by instigating hard core fundamentalist elements of Indian Muslim community. It is also believed that vulnerable youth are trained by ISI to destabilize India's internal security by spreading communal venom.
- Demographic factors: Demographic changes in Assam, West Bengal and the Kashmir Valley create opportunities for manipulation of communal sentiments for short-term political objectives.
- Social media factors: Negative impact of social media in spreading rumours, disinformation, hate-campaign and farming violence.
- Organized criminal involvement: Underworld criminals like Dawood Ibrahim, Chhota Shakeel, etc. are believed to have a key role in acting as agents of vested interest in instigating communal riots. There is also lack of political and social consciousness towards building a harmonious, coexistent society. We also need to build a nationalistic consciousness where the nation is above everything else.
- Lack of strong action: Lack of strong and decisive action by police and actions of biased or delayed action by them are also a cause. Real perpetrators are rarely punished and there is lack of fear of law that would prevent them from instigating communal riots.
- Poverty: Mass poverty and unemployment create a sense of frustration among the people. It generates backwardness, illiteracy, ignorance, etc. The unemployed youth of both the communities can be easily trapped by religious fundamentalists and fanatics. They are used by them to cause communal riots.
- Failure of Government: Both the Union and the State Governments often fail to prevent communalism in the country. Due to lack of prior information, they fail to take any preventive measures. The post-Godhra riot in Gujarat shows the inefficiency of the government to control the communal riot. Failure of immediate and effective steps has been a cause of the continuance of communalism.

Suggestion:

The following measures need to be implemented to curb the menace of communal violence:

- Taking pride in our heritage: The feelings of nationalism should be inculcated in the minds of people by reminding them about the glorious moments of freedom struggle wherein Hindus, Muslims and Sikhs were united in the fight against the British to safeguard the interests of the country.
- Impartial administration and police: Most riots persist for longer periods because people feel that the administration/police is not impartial. Changing this perception is most crucial for stopping riots. Perceived political interference in administration during communal violence must be eliminated. The directives of police reforms given by the Hon. Supreme Court should be adopted by state Governments in letter and spirit. A fixed tenure of District Magistrate/Deputy Commissioner and Superintendent of Police, SHO and Field officers will make a big difference.
- Policy of zero-tolerance towards violence: Government policy and practices should be firm and strict in this regard. It should not be affected by vote-bank politics. Police must take immediate, strong and effective action against those who indulge in violence irrespective of their community. There is an urgent need of not just an effective civil administration but also a speedy judiciary. Strict bail provisions must be made in cases of communal violence on the lines of the NDPS Act.

- ❑ Peace committees: Peace committees should be mandatory in every area. It should include secular and visionary people from all communities. People with high social standing like doctors, philanthropists and social workers must be engaged with such peace committees. Meetings of peace committee should be organized regularly. The district administration should engage actively with such committees to promote communal harmony.
- ❑ Win people's hearts through media and civil society: The faith of common people in the local police should be restored with the help of civil society, NGOs and media. Community policing and beat-constable system is also helpful in gathering intelligence and grass-roots information.
- ❑ Sensitise police towards feelings of minorities: The minority community at large views the police as communal and biased against them. Police must be sensitised to feelings of minorities and build trust.
- ❑ Holistic development of minority communities: There, should be a sincere effort to ensure that employment and skill development opportunities are available in the economic, educational and social spheres for the minority communities. Efforts should be made for bringing them in the mainstream of Indian society.
- ❑ Impart liberal values: Government should impart liberal values in our society through our education system. Soft skill development training should be provide to police and administration personnel.
- ❑ Strong legal action: The police should take adequate steps to identify in advance potential trouble makers and make timely use of preventive sections of law. Those inciting communal feelings must be punished. Provocative speeches by religious leaders in public and media must be dealt with strictly and strong legal action should be taken against them.
- ❑ Positive utilization of social media and mass media for awareness
- ❑ Proper checks and balances on social media
- ❑ Need to evolve early warning signals to prevent communal Mare ups.
- ❑ Ban on contesting elections: People charge sheeted in cases of communal violence should be banned from contesting elections.

Mob Violence

The rising incidents of these mob-lynching are due to following reasons:

- ❑ Lack of effective law and order - There are no stringent laws to penalise mob lynching. Lack of justice for victims further reinforces the vicious cycle of impunity. Also rather than taking swift action against perpetrators, law enforcement agencies act mostly against the victims themselves, booking them for violating cow protection laws.
- ❑ Promotions of communalism by vested interests - Lynchings are encouraged by the atmosphere of hate and suspicion created through sustained propaganda. Cow vigilantism, which is a pretext to exacerbate social conflicts between religious communities, serves the political purposes of ideologies.
- ❑ Senior ministers and elected representatives frequently come out in open defence of the attackers, charging the victims with provoking the attacks.
- ❑ Role of violence in Indian politics - Popular anger, outrage and violence are integral features of everyday politics in contemporary India. Thus mob feels empowered to take

Solution to mob-lynching

- ❑ The dastardly act of lynching has no easy solution. The responsibility of state legislatures should not be limited to enacting a law providing strict punishments. State legislatures need to be continuously involved with the issue. Their involvement should extend to an in-depth discussion with respect to budgetary requirements of police and judiciary and a continuous holding to account of the state administration for every unlawful act of lynching in the state.

- ❑ Stringent laws are not the only solution to a problem. They are part of the solution set and have to be supplemented with other measures. For maintaining law and order in the states, the most important requirement is that of an adequate, professional and responsive police force.
- ❑ Increase contact of police with local people - regular meeting of police personnel to local people's and children and youth in college could increase people's faith in police and administration.
- ❑ Awareness campaign and increase social media literacy by local administration with help of NGO.
- ❑ Police reforms, judicial reforms are essential to improve criminal justice system.
- ❑ Balanced regional growth should be ensured.

11-point prescription by Supreme Court to end mob lynching:

- ❑ The state governments shall designate a senior police officer in each district for taking measures to prevent incidents of mob violence and lynching.
- ❑ The state governments shall immediately identify districts, sub-divisions and villages where instances of lynching and mob violence have been reported in the recent past.
- ❑ The nodal officers shall bring to the notice of the DGP any inter-district co-ordination issues for devising a strategy to tackle lynching and mob violence related issues.
- ❑ It shall be the duty of every police officer to cause a mob to disperse, which, in his opinion, has a tendency to cause violence in the disguise of vigilantism or otherwise
- ❑ Central and the state governments should broadcast on radio and television and other media platforms including the official websites that lynching and mob violence shall invite serious consequence.
- ❑ Curb and stop dissemination of irresponsible and explosive messages, videos and other material on various social media platforms. Register FIR under relevant provisions of law against persons who disseminate such messages.
- ❑ Ensure that there is no further harassment of the family members of the victims.
- ❑ State governments shall prepare a lynching/mob violence victim compensation scheme.
- ❑ Cases of lynching and mob violence shall be specifically tried by designated court/fast track courts earmarked for that purpose in each district. The trial shall preferably be concluded within six months.
- ❑ To set a stern example in cases of mob violence and lynching, the trial court must ordinarily award maximum sentence upon conviction of the accused person.
- ❑ If it is found that a police officer or an officer of the district administration has failed to fulfill his duty, it will be considered as an act of deliberate negligence.

Armed Force Special Power Act (AFSPA)

Origin of AFSPA

- ❑ The Act came into force in the context of increasing violence in the Northeastern States decades ago, which the State governments found difficult to control. The Armed Forces (Special Powers) Bill was passed by both the Houses of Parliament and it was approved by the President on September 11, 1958. It became known as the Armed Forces Special Powers Act, 1958.
- ❑ Armed Forces (Special Powers) Acts (AFSPA), are Acts of the Parliament of India that grant special powers to the Indian Armed Forces in which each act terms "disturbed areas". According to The Disturbed Areas (Special Courts) Act, 1976 once declared 'disturbed', the area has to maintain status quo for a minimum of 3 months.

- ❑ One such Act passed on September 11, 1958 was applicable to the Naga Hills, then part of Assam. In the following decades it spread, one by one, to the other Seven Sister States in India's northeast (at present it is in force in Assam, Nagaland, Manipur excluding Imphal municipal council area, Changlang, Longding and Tirap districts of Arunachal Pradesh).
- ❑ Another one passed in 1983 and applicable to Punjab and Chandigarh was withdrawn in 1997, roughly 14 years after it came to force. An Act passed in 1990 was applied to Jammu and Kashmir and has been in force since.
- ❑ Presently AFSPA is enforced in the 6 states of North East and J&K. Tripura recently decided to lift this act.

Arguments against AFSPA

- ❑ It has been alleged that immunity granted by the act has led the armed forces to misuse the powers given to them by this act and commit offences like fake encounters and sexual assault.
- ❑ It leads to suspension of fundamental rights and liberties guaranteed to the citizens by the constitution. Thus it weakens democracy.
- ❑ Critics argue that this act has failed in its objective of restoring normalcy in disturbed areas although being in existence for about 50 years.
- ❑ Both Justice Verma Committee and Reddy Committee have recommended the removal of absolute immunity under AFSPA.
- ❑ On July 8, 2016, in a landmark ruling, The Supreme Court of India ended the immunity of the armed forces from prosecution under AFSPA, saying, in an 85-page judgment, "It does not matter whether the victim was a common person or a militant or a terrorist, nor does it matter whether the aggressor was a common person or the state. The law is the same for both and is equally applicable to both... This is the requirement of a democracy and the requirement of preservation of the rule of law and the preservation of individual liberties."
- ❑ Santosh Hegde commission on Manipur encounter deaths: The committee has suggested fixing a time frame of three months for the central government to decide whether to prosecute security personnel engaged in extrajudicial killings or unruly behaviour in insurgency-hit regions. The commission noted that AFSPA was an impediment to achieving peace in regions such as Jammu and Kashmir and the North East. The commission also said the law needs to be reviewed every six months to see whether its implementation is actually necessary in states where it is being enforced.
- ❑ Justice Jeevan Reddy Commission: The commission recommended to repeal AFSPA as "the Act is a symbol of hate, oppression and instrument of high handedness" but Government of India has not taken any decision in this direction.
- ❑ Second Administrative Reforms Commission: The second Administrative Reforms Commission (ARC) in its fifth report on "Public Order," recommended to repeal of Armed Forces Special Powers Act, 1958. It commented that its scrapping would remove sentiments of discrimination and alienation among the people of the North East India. The commission recommended to amend the Unlawful Activities (Prevention) Act, 1967 inserting a new chapter to deploy the armed forces of the Union in the North eastern States. It supported a new doctrine of policing and criminal justice inherent in an inclusive approach to governance.
- ❑ Supreme Court of India: Supreme Court said that any encounter carried out by armed forces in the garb of AFSPA should be subjected to thorough inquiry. In the words of Supreme Court "It does not matter whether the victim was a common person or a militant or a terrorist, nor does it matter whether the aggressor was a common person or the state. The law is the same for both and is equally applicable to both. This is the requirement of a democracy and the requirement of preservation of the rule of law and the preservation of individual liberties."

Arguments in favor of AFSPA

- It is essential for the armed forces to function effectively in insurgency and militancy affected areas.
- Provisions of this act have played a crucial role in maintaining law and order in disturbed areas. Thus protecting sovereignty and security of the nation.
- Hundreds of armed forces personnel lose their lives every year at the hands of insurgents and militants. It is crucial to empower them. Withdrawal would result in poor morale.
- In the absence of strict law, the armed forces will not be able to tackle the insurgent inside the country especially in the Kashmir and North eastern region of the country.

Bio-Terrorism

- Bioterrorism is the purposeful and premeditated deployment of dangerous microorganisms like bacteria, viruses, or their toxins to spread deadly diseases across a large area and decimate the local population.
- Deliveries of these agents include Scud missiles, spray-equipped cars, hand-pump sprayers, books or letters, weapons, remote controls, robots, etc. Monitoring the source of such illnesses or attacks is frequently challenging.

India needs bioterrorism legislation:

- India's high vulnerability: India is particularly susceptible to such attacks because of its dense population, limited access to healthcare, subtropical climate, lax hygienic practises, and inadequate sanitation facilities.
- Minimise the impact on society: By infecting vast populations with disease and causing widespread mortality, biological weapons have the ability to destabilise society in the shortest amount of time.
- Attacks have increased as a result of developments in biotechnology and nanotechnology, which have made more sophisticated biologic agents, in addition to the traditional germs, viruses, and poisons, freely accessible.

Preparedness to counter bio-terrorism:

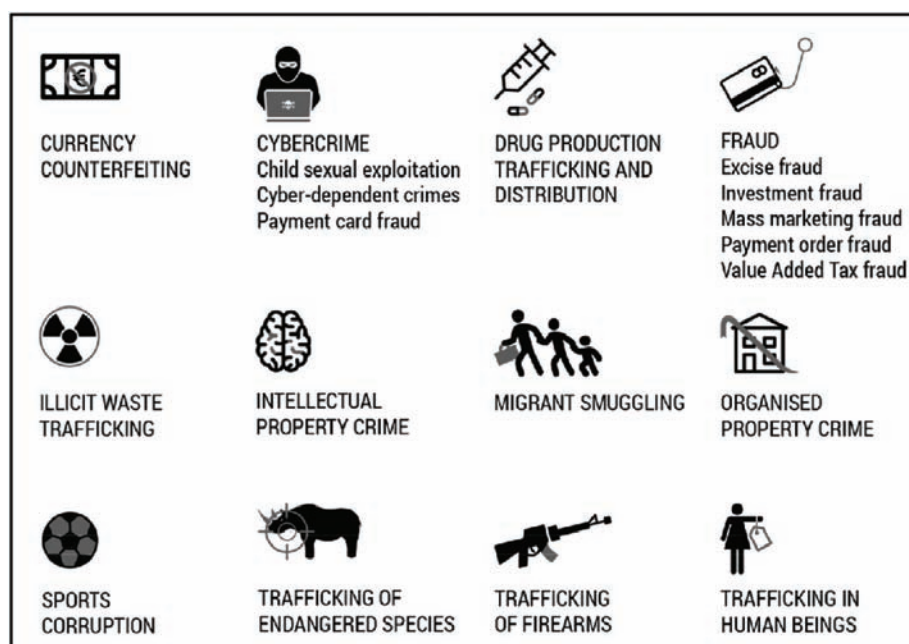
- It is necessary to reintroduce the Public Health (Prevention, Control and Management of Epidemics, Bioterrorism, and Disasters) Bill-2017, which provided definitions for the terms "epidemic," "isolation," "quarantine," and "social separation."
- One method to stop them is to look into the likelihood of bioterrorist attacks, train law enforcement personnel, and provide the required political and legal environment for better intelligence.
- Monitoring and analysis: It is feasible to spot the early warning signals of a biological warfare attack by spotting trends in non-specific disorders and analysing them.
- Laboratory investigation: For the lab and the entire institution, plans for the diagnosis and characterization of the biological entity must be devised.
- Medical management: It should provide services like chemotherapy that are preventive, educational, and curative in order to stop the disease from spreading.

Chapter 3

ORGANISED CRIME

- ❑ Organised crime means a structured group of three or more persons existing for some of time acting in concert with the aim of committing serious crimes or offences to obtain, directly or indirectly, financial or other material benefit.
- ❑ It manifests in many forms. Organised crime can be further classified into two categories, viz,
 - Traditional organised crime; and
 - Non-traditional (modern) organised crime.
- ❑ Traditional organised crime includes illicit liquor trade, betting, gambling, kidnapping, extortion, prostitution rackets, robbery, blackmailing, sand mafia, mining mafia, contract killing, pornography, etc.
- ❑ Non-traditional organised crime includes transnational crimes like money laundering, pumping fake Indian currency notes (FICN), hawala transfer, cybercrime, hacking, human trafficking, arms smuggling, drugs smuggling, etc.

Types of Organized Crime:



Similarity in the characteristics of organised crime and terrorism:

- ❑ Hierarchical structure
- ❑ Limited membership: - AL Qaida manual contains the qualification of members and Italian mafia only recruit Italian citizen.
- ❑ Violence to achieve goals
- ❑ Rules and regulations that defines behavior
- ❑ Specialization (division of labour)
- ❑ Desire to create monopoly

Nature of linkages of organised crime with terrorism:

- ❑ Activity appropriation: - use of similar methods without working together.
- ❑ Nexus: - each group relies upon support and expertise of others.
- ❑ Symbiotic relationship: - groups develop cooperative relationship to defend each other. Growing symbiosis makes both crime and terrorism powerful.
- ❑ Transformation: - from criminal to terrorist and from terrorist to criminal.

Shared tactics and methods of organized crime and terrorism:

- ❑ Internet and cyberspace are essential tools for recruitment, propaganda, planning, logistics, fund raising, money laundering.
- ❑ Other crimes include identity theft, video piracy, credit card fraud, phishing. Internet also serves as a platform to traffic women and children, smuggle illegal migrants, sell weapons, obtain assassination services, sell bomb making equipments, illegal drugs sell and to deal with toxic waste.
- ❑ Both profited from anonymity of internet to diffuse propaganda, extort victims and recruit new people.
- ❑ Prisons acts as meeting ground for organized crime and terrorism. It also helps in recruitment. The terrorists who executed the Madrid train bombings in 2004 were organized criminals that were recruited in prison by terrorists.
- ❑ Access to travel documents is as important as weapons because most acts of terrorism are facilitated by stolen identity.
- ❑ Shared tactics have resulted in strategic alliances between organized crime and terrorist groups, especially if they are operating in same territory.

Security implications of growing nexus between Terrorism and Organised Crime:

Impact	Direct impact	Indirect impact
Global security	▶ Protracted wars ▶ Weaken fragile states ▶ Weaken licit trade ▶ Weakens access to resources ▶ Retrenchment of globalization	▶ Human security ▶ Global health ▶ Global migration ▶ Greater economic disparity ▶ Greater pressure on resources ▶ Lower global GDP ▶ Destruction of biosphere ▶ Failed peacekeeping

Government	➤ Governance failure ➤ Failing and failed states ➤ Narco-states ➤ Kleptocracies ➤ Corrupt governments	➤ Lost of government revenues ➤ Trade imbalances ➤ Lost GDP ➤ Lost investments ➤ Reduction in tourism ➤ Shift of power to criminal gangs ➤ Prevents human development
Society/ human security	➤ Erosion of trust in government ➤ Exposure to crime/violence ➤ Illegal trade ➤ High risk environments (pollution, drugs, arms) ➤ Loss of legal business revenues ➤ Kidnapping/extortion/murder ➤ Illegal trafficking of men/women/children ➤ Natural resources/wildlife/arms	➤ Rise of populist and criminal groups ➤ Reduction of resources (food, oil, water, land) ➤ Higher cost of living ➤ Higher drug addiction and increase in HIV/AIDS

Linkage of Terrorism and Organized Crime in India

- ❑ There is a linkage between terrorism and organized crime. An organized crime group cannot exist without an extensive peripheral network. Which involves the bankers, politicians and the police; basically the portals into the illicit world that protects the core of the organized crime group and revolves around business activity. With such a network, territorial possessions come into play, and popular support is needed. It doesn't necessarily mean that the population condones the violence committed by the cartels but it does mean that the cartels, can effectively intimidate the population to tolerate activity and allow business to go up on as usual.
- ❑ By contrast, a terrorist group does not need to rely on an extensive network. By definition, terrorism is primarily driven by political aims. The financial aspect of their activities are a means to an end, so this places very different constraints on the terrorist group and allows the terrorist groups to engage in much bolder, riskier, and violent acts than an organized crime group would.
- ❑ In India, the linkages between the two exist at national and transnational levels. At the national level, both terrorists and those involved in organized crime are within India.
- ❑ In the North-east, numbers of insurgent groups over a time have morphed into crime syndicates. All militant groups run a similar government or have their areas of influence involved in collecting money directly from the people, and from government funds due to misgovernance. Government officials are threatened or bribed to award contracts and thus, important commodities like rice and kerosene are sold to the public at much higher prices. There are growing number of extortion, kidnap, contracts, black marketing transnational drugs and arms to finance terrorism.
- ❑ Other linkage is through the spread of fake currency. Terrorists are the main agent of these crimes. The Indian mujahidin resorted to crime to raise funds. This includes robberies and kidnapping. Maoists terror movements also use coercion, robberies of bank and kidnapping to collect huge funds.
- ❑ Thus, the intersection of criminal networks and terrorist organizations can be broadly grouped into three categories - co-existence (they coincidentally occupy and operate in the same geographic space at the same time), cooperation (they decide that their mutual interests are both served, or at not least

severely threatened, by temporarily working together) and convergence (each begins to engage in behavior(s) that is/are more commonly associated with the other).

Steps Undertaken by India:

- ❑ Statutory Measures: India has enacted Narcotics Drugs and Psychotropic Substances Act, 1985 (NDPS Act) and Prevention of Illicit Trafficking of Narcotics Drug and Psychotropic Substances Act, 1988 through which the country is addressing various aspects of drug problems.
- ❑ International Conventions: India is signatory to all three UN Conventions namely, the Single Convention on Narcotics Drugs 1962, the 1971 UN Convention on Psychotropic Substances, and the 1988 UN Convention against Illicit Trafficking of Narcotics Drugs, Psychotropic Substances and has also supported the global efforts led by the UN office on Drug and Crime (UNODC) to curb the perpetrating drug menace.
- ❑ Inter-Governmental Initiatives: India has entered into various arrangements like Bilateral Agreements, Memorandum of Understandings with Nepal, Thailand, and Myanmar, Joint Working Groups on Counter. Terrorism and Judicial Cooperation with the countries in the region.
- ❑ India has formulated a National Policy on Narcotics Drugs and Psychotropic Substances which has given equal emphasis on supply and demand reduction.
 - New guidelines for grant of rewards to be paid to officers, informers and other persons in case of seizures of Narcotics drugs, Psychotropic substances were also issued recently.
 - Ensuring physical security of the borders and coasts by strengthening patrolling and surveillance.
- ❑ The National Security Act 1980 provides for preventive detention by the Central Government or the State Government, or by the officers designated by them.
- ❑ The detention order is issued for one year with a view to preventing a person from acting in any manner prejudicial to the defence of India, or to the friendly relations with foreign powers.
- ❑ The expression 'Security of India' is open to liberal interpretation, and this Act has been used, though sparingly, against anti-national elements and hard core gangsters.
- ❑ Detention is an executive action or when the case does not go to the court for trial.
- ❑ The Prevention of Illicit Traffic in Narcotic Drugs and Psychotropic Substances Act 1988 provides for detention of persons related with Illicit Traffic in Narcotic Drugs and Psychotropic Substances.
- ❑ The Central Government or the State Government or the designated officers of these Government, can pass an order for detaining a person with a view to preventing him from engaging in illicit traffic in narcotic drugs.
- ❑ Anti-Trafficking Nodal Cell has been set up by MHA to act as a focal point for communicating various decisions and to follow up on action taken by the state governments to combat human trafficking.
- ❑ The Ministry of Women and Child Development funds NGO-run shelters and rehabilitation services for women and children through the Ujjawala program, specifically for female sex-trafficking victims, and the Swadhar program for women in difficult circumstances.
- ❑ The government has also signed agreements with Bangladesh, Nepal, and Bahrain, etc. to curb trafficking.
- ❑ The government recently introduced "The Trafficking of Persons (Prevention, Protection and Rehabilitation) Bill, 2018 in Lok Sabha.

UN Convention against Transnational Organized Crime and the Protocols

- ❑ This is the only international convention, which deals with organised crime. It is a landmark achievement, representing the international community's commitment to combating transnational

organised crime and acknowledging the UN's rule in supporting this commitment. The adoption of the Convention at the fifty-fifth session of the General Assembly of the United Nations in 2000 and its entry into force in 2003 also marked a historic commitment by the international community to counter organised crime.

Terror Financing

- ❑ Terrorists require money to operate. Without funding, they cannot purchase weapons, equipment, supplies, or services. The source of terrorist funds may be licit or illicit, and funding often takes the form of multiple small donations, rather than one large sum of money.
- ❑ Terrorist groups may be directly or indirectly linked to organized criminal groups and may engage in criminal activities, including drugs or arms trafficking, extortion, and kidnapping for ransom. Terrorism financing is a global phenomenon that not only threatens Member States' security, but can also undermine economic development and financial market stability.

Strategy to deal with the terror financing

- ❑ In dealing with financing of terrorist activities, the emphasis has to be more on obstructing such activities while in progress. The main planks of a strategy to deal with the financial aspects of terrorist activities should involve:
 - Asset recovery and obstruction powers.
 - Legal penalties against persons/organizations involved in financing terrorism.
 - Adoption of diligent customer identification programmes, and standard record keeping procedures by financial institutions/agencies.
 - Reporting of suspicious financial activity by individuals and institutions.
 - Anti-money laundering measures.
 - Capacity building and coordination mechanisms between agencies involved.
 - International cooperation.

Steps taken by Government to block the flow of funds for Financing Terrorist Activities

- ❑ Making terrorist finance an offence: Under TADA and POTA, holding property derived or obtained from any terrorist activity or acquiring them through terrorist funds was an offence.
- ❑ Demonetisation : The government targeted the fake currency notes in circulation, which are an important source of terror financing. As per a study, Rs. 70 crore in fake currency notes were pumped into the economy every year.
- ❑ Improved Safety features in currency: The new notes will be difficult to be faked as they have advanced safety features.
- ❑ Strengthening of PMLA: In 2013 by incorporating the provisions relating to removing the monetary threshold for schedule offences, strengthening confiscation, and provisional attachment powers with regard to money laundering investigation, covering new financial institutions, and designated non-financial business and professions within the scope of PMLA.
- ❑ A special Combating Financing of Terrorism (CFT) Cell has been created in the Ministry of Home Affairs in 2011, to coordinate with the Central Intelligence/Enforcement Agencies, and the State Law Enforcement Agencies for an integrated approach to tackle the problem of terror funding.

- ❑ A Terror Funding and Fake Currency Cell was set up in the National Investigation Agency to investigate Terror Funding cases.

Drug Trafficking

- ❑ India is one of the top opiate consumer markets in the world, making it susceptible to an increase in supply.
- ❑ There are already indications that opiate trafficking from Afghanistan may become more intense, moving not only south and west along the old Balkan route, but also possibly eastward.
- ❑ Over the past ten years, there have been 284 million more drug users worldwide, a 26 percent rise (15-64 years). 11.2 million Injected medicines, on average. One million people had HIV, 1.4 million had hepatitis C, and 1.2 million had both.
- ❑ 209 million people use marijuana globally, 61 million use opiates, 34 million use amphetamines, 21 million use cocaine, and 20 million use ecstasy. While opium addiction was widespread in south-eastern Europe and central Asia, cannabis misuse was treated most frequently in Africa, South and Central America, and Central Asia.
- ❑ The use of cocaine, methamphetamine, and opium has all increased. The global production of cocaine increased 11% to 1,982 tonnes in 2020 despite the COVID-19 epidemic, while seizures increased to a record 1,424 tonnes.

World Drug Report:

- ❑ The UNODC (United Nations Office on Drugs and Crime) released the report in Vienna. The global drug markets are thoroughly examined in the World Drug Report 2022. Within the context of the Sustainable Development Goals, climate change, and environmental sustainability, it investigates the relationship between pharmaceuticals and the environment.

United Nations Office on Drugs and Crime:

- ❑ It was founded in 1997, and in 2002 it was given the name United Nations Office on Drugs and Crime (UNODC). By combining the United Nations International Drug Control Program (UNDCP) and the Crime Prevention and Criminal Justice Division of the United Nations Office at Vienna, it serves as the Office for Drug Control and Crime Prevention.

Related International Initiatives:

- ❑ The 26th of June is designated as International Day against Drug Abuse and Illicit Trafficking. Single Narcotic Drug Convention of 1961 The 1971 Psychotropic Substances Convention. 1988's UN Convention against the Illicit Trade in Narcotic Drugs and Psychotropic Substances All three are ratified by India, which also passed the Narcotics Drugs and Psychotropic Substances (NDPS) Act in 1985.

Indian vulnerability:

- ❑ India is particularly vulnerable to drug trafficking since it is located between the two main opium-producing regions of the world: the "Golden Crescent" and the "Golden Triangle." Pakistan, Iran, and Afghanistan make up the Golden Crescent region in the South. The junction of the Mekong and Ruak rivers, which separates Thailand from Cambodia, is known as the Golden Triangle.



Chapter 4

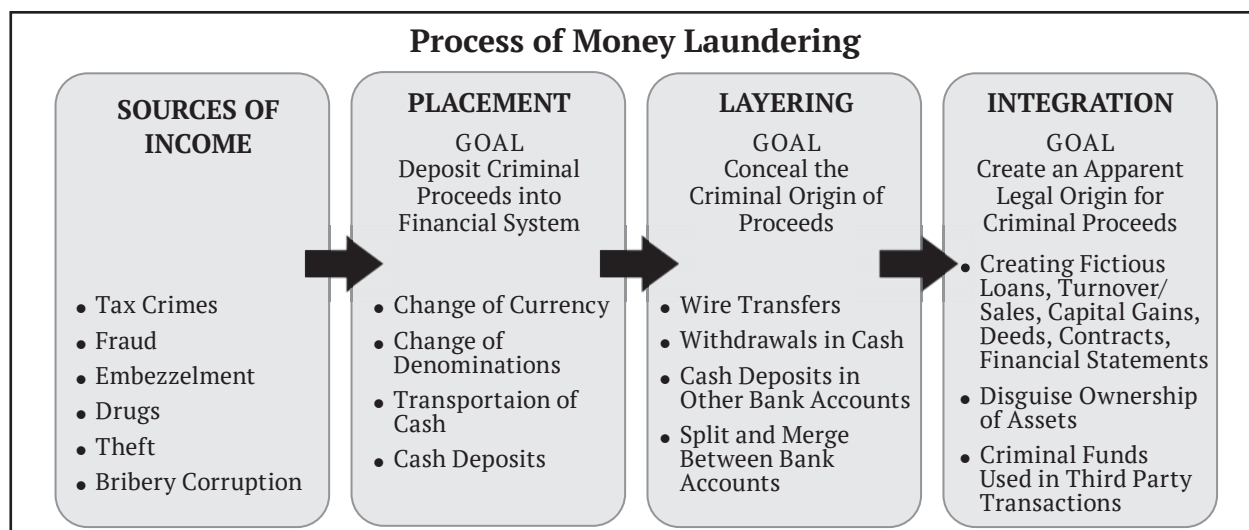
MONEY LAUNDERING & BLACK MONEY

- ❑ Money laundering is the illegal process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking transfers or commercial transactions. The overall scheme of this process returns the money to the launderer in an obscure and indirect way. In other words, money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source. The most common types of criminals who need to launder money are drug traffickers, embezzlers, corrupt politicians and public officials, mobsters, terrorists and con artists.
- ❑ Many jurisdictions have set up sophisticated financial and other monitoring systems to enable law enforcement agencies detect suspicious transactions or activities, and many have set up international cooperative arrangements to assist each other in these endeavors. The United Nations Office on Drugs and Crime (UNODC) estimates that the “amount of money laundered globally in one year is 2–5% of global GDP, or \$800 billion – \$2 trillion in current US dollars.”

How is money laundered?

- ❑ Traditionally, money laundering has been described as a process which takes place in three distinct stages:

The basic money laundering process has three steps



Negative Effects of Money Laundering

- ❑ Money Laundering threatens national governments and international relations between them through corruption of officials and legal systems. It undermines free enterprise and threatens financial stability by crowding out the private sector, as legitimate businesses cannot compete with the lower prices for goods and services that businesses using laundered funds can offer.
- ❑ There are few specific challenges which is posed by money-laundering activities throughout the world.
- ❑ **Terrorism:** Money Laundering serves as an important mode of terrorism financing. Terrorists have shown adaptability and opportunism in meeting their funding requirements. Terrorist organizations raise funding from legitimate sources, including the abuse of charitable entities or legitimate businesses or self financing by the terrorists themselves. Terrorists also derive funding from a variety of criminal activities ranging in scale and sophistication from low-level crime to organized fraud or narcotics smuggling or from state sponsors and activities in failed states and other safe havens.
- ❑ **Threat to Banking System:** Across the world, banks have become a major target of money laundering operations and financial crime because they provide a variety of services and instruments that can be used to conceal the source of money. With their polished, articulate and disarming behaviour, money launderers attempt to make bankers lower their guard so as to achieve their objective.
- ❑ **Threat to Economic Stability:** An IMF working paper concludes that money laundering impacts financial behaviour and macro-economic performance in a variety of ways, including policy mistakes due to measurement errors in national account statistics, volatility in exchange and interest rates due to unanticipated cross border transfer of funds, the threat of monetary instability due to unsound asset structures, effects on tax collection and public expenditure allocation due to misreporting of income and many more such ways.

Other economic impact

- ❑ Discourages foreign investors
- ❑ Encourages tax evasion culture
- ❑ Results in exchange and interest rates volatility
- ❑ Undermining of the integrity of financial markets: The succeeding reputational loss by financial institutions results in a loss of confidence by consumers in these affected financial institutions who may be perceived to be involved in fraudulent activities.
- ❑ Loss of revenue: money laundering decreases the tax funds available for collection in the economy and by implication government's revenues. Consequently, governments may have to levy higher taxes in order to obtain the funds necessary to fulfill their responsibilities towards their citizens.
- ❑ Reputation risk: nations that are competing as destinations for legitimate investments may face difficulty to do so if there is a perception that the country has a poor track record of dealing with money laundering or is seen to be a centre for money laundering. This is because legitimate investors are wary of being associated with any country that has a negative reputation.

Social Impacts:

- ❑ Increased criminality
- ❑ Decreases human development
- ❑ Misallocation of resources
- ❑ Affects trust of local citizens in their domestic financial institutions
- ❑ Declines the moral and social position of the society by exposing it to activities such as drug trafficking, smuggling, corruption and other criminal activities

Political Impacts:

- Initiates political distrust and instability
- Criminalization of politics

Challenges in tackling money laundering

- Growth of Technology: The enforcement agencies are not able to match up with the speed of growing technologies which makes processes such as placement, layering and integration even more complicated.
- Non-fulfillment of the purpose of KYC Norms: KYC norms do not cease or abstain from the problem of Hawala transactions as RBI cannot regulate them. Further, such norms are only a mockery as the implementing agencies are indifferent to it. Also, the increasing competition in the market is forcing the Banks to lower their guards and thus facilitating the money launderers to make illicit use of it in furtherance of their crime.
- Widespread act of smuggling: there are a number of black market channels in India for the purpose of selling goods offering many imported consumers goods such as food items, electronics etc. which are routinely sold.
- Lack of comprehensive enforcement agencies: Separate wings of law enforcement agencies dealing with money laundering, cyber crimes, terrorist crimes, economic offences etc lack convergence among themselves.
- Tax Heaven Countries: They have long been associated with money laundering because their financial secrecy laws allow the creation of anonymous accounts while prohibiting the disclosure of financial information.

Measures Taken by the Government to prevent Money laundering

- Constitution of the Special Investigation Team (SIT) on Black Money under Chairmanship and Vice-Chairmanship of two former Judges of the Supreme Court
- Enactment of a comprehensive law, 'The Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015 to specifically deal with black money stashed away abroad
- Constitution of Multi-Agency Group (MAG) consisting of officers of Central Board of Direct Taxes (CBDT), Reserve Bank of India (RBI), Enforcement Directorate (ED), and Financial Intelligence Unit (FIU) for investigation of recent revelations in Panama paper leaks.
- Proactively engaging with foreign governments with a view to facilitate and enhance the exchange of information under Double Taxation Avoidance Agreements (DTAAs)/Tax Information Exchange Agreements (TIEAs)/Multilateral Conventions.
- Enabling attachment and confiscation of property, equivalent in value, held within the country where the property/proceeds of crime is taken or held outside the country by amending the Prevention of Money-laundering Act, 2002 through the Finance Act, 2015.
- Enactment of the Benami Transactions (Prohibition) Amendment Act, 2016 to amend the Benami Transactions (Prohibition) Act, 1988 with a view to, inter alia, enable confiscation of Benami property and prosecution of benamidar and the beneficial owner.
- Initiation of the information technology based 'Project Insight' for strengthening the non-intrusive, information driven approach for improving tax compliance.
- Launching of 'Operation Clean Money' in 2017 for collection, collation, and analysis of information on cash transactions, extensive use of information technology and data analytics tools for identification of high risk cases, expeditious e-verification of suspect cases and enforcement actions in appropriate cases, which include searches, surveys, enquiries, assessment of income, levy of taxes, penalties, etc.

The Prevention of Money Laundering Act, 2002 (PMLA)

- The Prevention of Money Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. It came into force in 2005. PMLA defines money laundering offence and provides for the freezing, seizure, and confiscation of the proceeds of crime. Salient Features of this act are as follows:
 - RBI, SEBI and IRDA have been brought under the PMLA, and therefore the provisions of this act are applicable to all financial institutions, banks, mutual funds, insurance companies, and their financial intermediaries.
 - The agency monitoring the anti-money laundering activities in India is the Financial Intelligence Unit (FIU-IND). This unit is responsible for receiving, processing, analysing, and disseminating information relating to suspect financial transactions. FIU-IND is also responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC), headed by the Finance Minister.
 - Punishment for offence of money laundering can be of imprisonment upto 3-7 years with fine upto 5 lakh rupees. But in case of offences done under Narcotic Drugs and Psychotropic Substance Act 1985, the maximum punishment is to the extent of 10 years rather than 7 years.
 - Obligation of banking companies, financial institutions and intermediaries: Banking companies have to follow the procedure of KYC Norms (Know your customer) Maintain the records for nature and value of the transaction to be transacted, whether such transaction was singly transacted or was a part of a series of transaction taken place in a month.
 - Maintain record for a period of 10 years from the date of cessation of transaction between the clients and the banking company, or financial institution or intermediary, as the case may be.
 - Furnish information of above transaction to director within the prescribed time.
 - Verify and maintain the records of identity of all clients in respect of such transactions to Director within the prescribed time.

The Prevention of Money Laundering (Amendment) Act 2012

- The PMLA was enacted in 2002, but was amended thrice, first in 2005, then in 2009 and then 2012. The 2012 version of the amendment received the President's assent on 3rd January 2013, and the law became operational from February 15, when the finance ministry notified it. PMLA (Amendment) Act, 2012 has enlarged the definition of money laundering by including activities such as concealment, acquisition, possession and use of proceeds of a crime. Some other features are as follows:
 - The amendment has introduced the concept of corresponding law to link the provisions of Indian law with the laws of foreign countries, and to provide for transfer of the proceeds of foreign predicate offence committed in any manner in India.
 - It also adds the concept of 'reporting entity' which would include a banking company, financial institution, intermediary, or a person carrying on a designated business or profession. The Prevention of Money Laundering Act, 2002 levied a fine upto Rs 5 lakh. The amendment act has removed this upper limit.
 - The act has provided for provisional attachment and confiscation of property of any person (for a period not exceeding 180 days).

Recent changes in anti-money laundering process

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

New amendment

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

Financial Intelligence Unit – India (FIU-IND)

- ❑ FIU-IND is responsible for coordinating and strengthening efforts of national and international intelligence, investigation and enforcement agencies in pursuing the global efforts against money laundering and related crimes. FIU-IND is an independent body reporting directly to the Economic Intelligence Council (EIC) headed by the Finance Minister.

Enforcement Directorate (ED):

- ❑ It is a law enforcement agency and economic intelligence agency responsible for enforcing economic laws and fighting economic crime in India.
- ❑ One of the main functions of ED is to Investigate offences of money laundering under the provisions of Prevention of Money Laundering Act, 2002(PMLA).
- ❑ It can take actions like confiscation of property if the same is determined to be proceeds of crime derived from a Scheduled Offence under PMLA, and to prosecute the persons involved in the offence of money laundering.

Global initiatives to curb money laundering

- ❑ The Vienna convention: It was the first major initiative in the prevention of money laundering held in December 1988. This convention laid down the groundwork for efforts to combat money laundering by obliging the member states to criminalize the laundering of money from drug trafficking.
- ❑ Basle committee’s statement of principles: In December 1988, the Basle Committee on Banking Regulations and Supervisory Practices issued a statement of principles which aims at encouraging the banking sector to adopt common position in order to ensure that banks are not used to hide or launder funds acquired through criminal activities.
- ❑ THE FINANCIAL ACTION TASK FORCE (FATF): The FATF is an inter-governmental body established at the G7 summit at Paris in 1989 with the objective to set standards and promote effective implementation of legal, regulatory and operational measures to combat money laundering and terrorist financing and other related threats to the integrity of the international financial system
- ❑ UNITED NATIONS GLOBAL PROGRAMME AGAINST MONEY LAUNDERING (UNGPM): GPM was established in 1997 with a view to increase effectiveness of international action against money laundering through comprehensive technical cooperation services offered to Governments.
- ❑ Egmont Group Membership: Financial Intelligence Unit-India (FIU-IND) is a member of the Egmont Group, an international organization for stimulating co-operation among FIUs. The Egmont Group serves as an international network fostering improved communication and interaction among FIUs. The goal of the Egmont Group is to provide a forum for FIUs around the world to improve support to their respective governments in the fight against money laundering, terrorist financing and other financial crimes.
- ❑ Eurasian Group (EAG) Project: Eurasia Group EAG is a FATF styled Regional Body (FSRB). It is the world’s leading global political risk research and consulting firm. According to the EAG Terms of Reference its primary objectives include money laundering and financing of terrorism typologies analysis and exchange of experience in combating such crimes with regard to regional peculiarities.

Black Money in India

Black money is a term used in common parlance to refer to money that is not fully legitimate in the hands of the owner. This could be for two possible reasons. The first is that the money may have been generated through illegitimate activities not permissible under the law, like crime, drug trade, terrorism, and corruption, all of which are punishable under the legal framework of the state. The second and perhaps more likely reason is that the wealth may have been generated and accumulated by failing to pay the dues to the public exchequer in one form or other. There is no doubt that manifestation of black money in social, economic and political space of our lives has a debilitating effect on the institutions of governance and conduct of public policy in the country. Governance failure and corruption in the system affect the poor disproportionately. The success of an inclusive development strategy critically depends on the capacity of our society to root out the evil of corruption and black money from its very foundations. Our endeavour in this regard requires a speedy transition towards a more transparent and result oriented economic management systems in India.

Black money estimates

- ❑ No clear estimate of black money owned by Indians and stashed abroad is available.
- ❑ Various studies and estimates have pegged black money circulation in India anywhere between 7 per cent and 120 per cent of the country's gross domestic product (GDP).
- ❑ Between 2008 and 2012, various reports quoted anywhere between \$500 billion and \$1.5 trillion relying on estimates of a Swiss Bankers Association (SBA) report.
- ❑ In 2019, the National Institute of Financial Management reported to the Lok Sabha Standing Committee on Finance, that the estimate is about \$216 billion-\$490 billion.

Causes of Black Money in India

- ❑ Prohibition causes black money: Certain activities are usually forbidden by law such as gambling, production of illicit liquor, smuggling, trafficking illegal drugs, lending at exorbitant interest charges, money lending without proper license etc. When some individuals wish to undertake these activities, these will apparently go unreported and incomes so earned would be totally black.
- ❑ Political Funding encourages black money: Political funding in India also causes a significant amount of black income. Our election laws and behavior of political parties are primarily responsible for this. Today contesting of elections has become a very costly affair.
- ❑ Inflation leads to black money: The genesis of black money can also be found in the persistent inflation in the country, which has enhanced incentives and opportunities to earn such incomes.
- ❑ Deficiencies of the Tax System pays way for black money: There are various lacunae in the tax system that encourages generation of black income. First, high personal Income Tax Rates cause people to try and evade taxes, and thus lead to generation of black income. The dilemma for the Government is that even efforts at lowering tax rates do not lead to larger payments of income tax by the higher income groups.
- ❑ Although there are a number of tax laws pertaining to income tax, sales tax, stamp duties, excise duties etc. enforcement is weak due to widespread corruption in these departments.
- ❑ Quotas, Controls and Licences generates black money: The "License, Quota, Permit Raj" that has dominated the Indian system of controls has often led to the initiation of various ways of escaping these and thus, the generation of black income.
- ❑ Ineffective Enforcement of Tax Laws gives way for black money: Ineffective enforcement of tax laws is also a cause for black money. Lack of proper training and inefficiency of the department people led to the creation of black money.

Negative Effects of Black Money

- ❑ **Dual Economy:** The increase in the amount of black money in India over a period of time lead to the perpetual growth of economic dualism which consists of Parallel economy (black money economy) operating side by side with the Official or Reported economy on the country.
- ❑ **Under-estimation:** A large underground economy and growth of black income lead to under-estimation of the true size and incorrect picture of the economy by the officially complied national income data.
- ❑ **Loss of Revenue to the Government:** Black money is largely attributed to tax evasion. Its direct impact is the loss of the Government revenue.
- ❑ **Undermining the Equity:** When the Government resorts to progressive direct taxation to maintain equity in the distribution of the tax burden, the tax evasion and growth of black money affect the very concept of social justice by not allowing the desirable reduction in inequalities of incomes.
- ❑ **Widening the Gap between the Rich and the Poor:** Growth of the black economy causes regressive distribution of income in the society.
- ❑ **Lavish Consumption Spending:** Black money is disposed off by lavish spending on travels and tours, entertainment, ostentatious articles, financing of extravagant elections etc. This has also lead to many social evils and deteriorated the values of life of the common people.
- ❑ **Distortion of Production Pattern:** The black money has altered the choice coefficients in the market in favor of luxuries, which lead to the diversification of productive resources from essential goods to the non-essential goods.
- ❑ **Distribution of Scarce Resources:** Black money holders are always in a position to put their prior claim over the scarce goods in the market due to their readiness and ability to pay more, thereby depriving the honest and poor people from their legitimate share. This obviously reduces the net economic welfare of the Indian society at large.
- ❑ **Deteriorate the General Moral Standards of the Society:** Black money is largely responsible for the deterioration of general moral standards of the society.
- ❑ **Average Effect on Production:** As a consequence, the consumption pattern is titled in favor of the rich and elite, at the cost of encouraging production of articles of mass consumption.
- ❑ **The part of black money invested in unproductive channels like holding of gold, contributes nothing or very little to productive activities.**
- ❑ **Presence of black money results in the flight of funds from India to foreign countries through clandestine channels.** The flight of capital abroad lowers productivity and employment potential within the country.
- ❑ **Black money is used for crimes or anti-social activities.** In heinous crimes against the society, like terrorism, what is used is black money. This is the most serious consequence.

Steps taken by government to curb black money

- ❑ **Amendment to Benami properties transaction act:** To provide with a wider definition to Benami properties and to provide with robust structural mechanism to deal with black money.
- ❑ **Promoting Cashless Economy:** So as to ensure better control over money flow in the economy and prevent creation of black money.
- ❑ **Special Investigation team under Justice Shah:** To unearth the black money stacked in the country.
- ❑ **Demonetisation:** To bring out the black money or flush it out of the economy by making it redundant.
- ❑ **Transparency in political funding:** By limiting the anonymous cash donations to Rs 2000 and introduction electoral bonds to prevent entry of black money in politics.
- ❑ **Enactment of the Black Money (Undisclosed Foreign Income and Assets) and Imposition of Tax Act, 2015** to more effectively tackle the cases involving black money stashed abroad.

- ❑ Enactment of the Benami Transactions (Prohibition) Amendment Act, 2016 to effectively deal with domestic black money cases.
- ❑ In order to check creation of shell companies which are incorporated outside but controlled from India, the concept of 'Place of Effective Management' (POEM) for determination of residence of a company incorporated in a foreign jurisdiction, has been introduced in the Finance Act, 2016
- ❑ Constitution of the Special Investigation Team (SIT) on Black Money in May, 2014 under Chairmanship and Vice-Chairmanship of two former Judges of Hon'ble Supreme Court.
- ❑ Constitution of Multi-Agency Group (MAG) for coordinated and effective investigation in 'Panama paper leaks' cases and Paradise Leaks cases.
- ❑ Task Force (TF) on Shell Companies constituted under the joint chairmanship of Revenue Secretary and Secretary (Ministry of Corporate Affairs) in February, 2017.
- ❑ Operation Clean Money initiated by the Income Tax Department.

Various other anti-evasive legislative measures taken:

- ❖ Legislative Framework:
 - Prevention of Money Laundering Act, 2002)
 - Benami Transactions Prohibition Act, 1988)
 - Lokpal and Lokayukta Act)
 - Prevention of Corruption Act, 1988)
 - The Undisclosed Foreign Income and Assets (Imposition of Tax) Bill, 2015

Post-demonetization, significant measures:

- ❑ Quoting of PAN made mandatory for all cash deposits above Rs. 50,000 and aggregating to more than Rs. 2.5 lakh.
- ❑ Further, Rule 114E of the Income Tax Rules, 1962 was amended to mandate the prescribed reporting entities to report all cash deposits above Rs. 2.5 Lakhs in savings accounts and Rs. 12.5 Lakhs in current account during the above period.
- ❑ Restriction on cash transaction of Rs. 2 lakh or more (Section 269ST of I. T. Act), no deduction under section 80G if cash donation exceeds Rs. 2000, restriction on donations of Rs.2000/- or more to political parties otherwise than by a bank account or through electoral bonds.
- ❑ Deeming fair market value as full value of consideration for computation of capital gains in case of transfer of shares other than quoted shares.
- ❑ Mandating that a person who has an account (other than a time deposit and a Basic Saving Bank Deposit Account) maintained with a banking company or a cooperative bank shall furnish his PAN or Form No. 60 etc.
- ❑ Linking of Aadhar with PAN has been made mandatory for filing Income Tax Returns and for applying for new PAN from July 2017.

International Cooperation:

- ❑ Proactively engaging with foreign governments to enhance the exchange of information (EoI) under tax treaties, India has tax treaties with 148 foreign jurisdictions. E.g. Foreign Account Tax Compliance Act with the US.
- ❑ India joined a group of 48 countries as early adopters to new global standards for automatically exchanging information from 2017.
- ❑ India-Mauritius and India-Singapore tax treaties amended to adopt source based taxation of capital gains with a view to help curb tax evasion and tax avoidance.

- ❑ The Government of India has also joined the Multilateral Competent Authority Agreement (MCAA) for Automatic Exchange of Information as per Common Reporting Standards (CRS).

Pradhan Mantri Garib Kalyan Yojana, 2016 (PMGKY)

- ❑ The Taxation Laws (Second Amendment) Act, 2016 was enacted, which enabled levy of tax at a higher rate on the undisclosed income under which a person could declare his undisclosed cash by paying tax, surcharge & penalty totaling to 50% of the undisclosed income. Besides, he would have to keep 25% of the undisclosed income in Pradhan Mantri Garib Kalyan Deposit Scheme, interest free for 4 years.

Judicial Efforts

- ❑ On the directions of the Supreme Court, the government in May 2014 constituted the Special Investigation Team (SIT) on black money.

Suggestions to prevent Indian black money

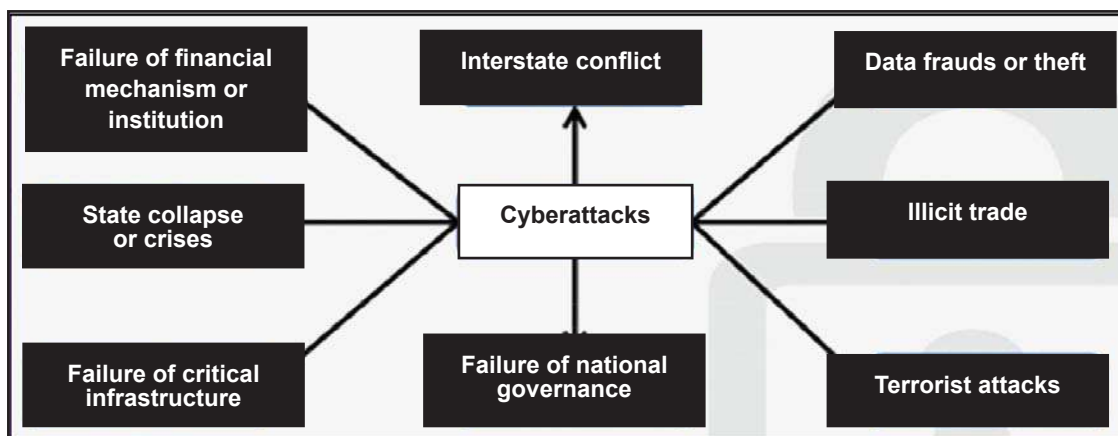
- ❑ Reducing disincentives against voluntary compliance: Excessive tax rates increase black money and tax evasion. When tax rates approach 100 per cent, tax revenues approach zero, because higher is the incentive for tax evasion and greater the propensity to generate black money. Lower taxes and simpler compliance process reduces black money, suggests the white paper.
- ❑ Economic liberalization: The process of economic liberalisation must be relentlessly continued to further remove underground economy and black money, suggests the report.
- ❑ Reforms in vulnerable sectors of the economy: Certain vulnerable sectors of Indian economy are more prone to underground economy and black money than others. These sectors need systematic reforms. As example, gold trading, which was one of the major sources of black money generation and even crime prior to the reforms induced in that sector. While gold inflows into India have remained high after reforms, gold smuggling is no longer the menace as it used to be.
- ❑ Creating effective credible deterrence: Effective and credible deterrence is necessary in combination with reforms, transparency, simple processes, elimination of bureaucracy and discretionary regulations.
- ❑ International enforcement: India has Double Tax Avoidance Agreements with 82 nations, including all popular tax haven countries. Of these, India has expanded agreements with 30 countries which require mutual effort to collect taxes on behalf of each other, if a citizen attempts to hide black money in the other country. The Agreements be expanded to other countries as well to help with enforcement.

Chapter 5

CYBER SECURITY

- ❑ Technology of today has advanced to the extent that doctors can diagnose diseases when patient is sitting at home watching TV, communicate with friends across the world in few seconds, pay bills just by clicking a button. Though the benefits are great but also one should consider or think about the complexities and dangers.
- ❑ Research says, more than 50% of onliners are victim of some form of cyber crime every year, which includes computer viruses, malware, credit card fraud, online scams, phishing, and identity theft and so on. These crimes will lead the country to lose millions of rupees or dollars, also time and expenses to put back the things in right directions.

Cyber Threats



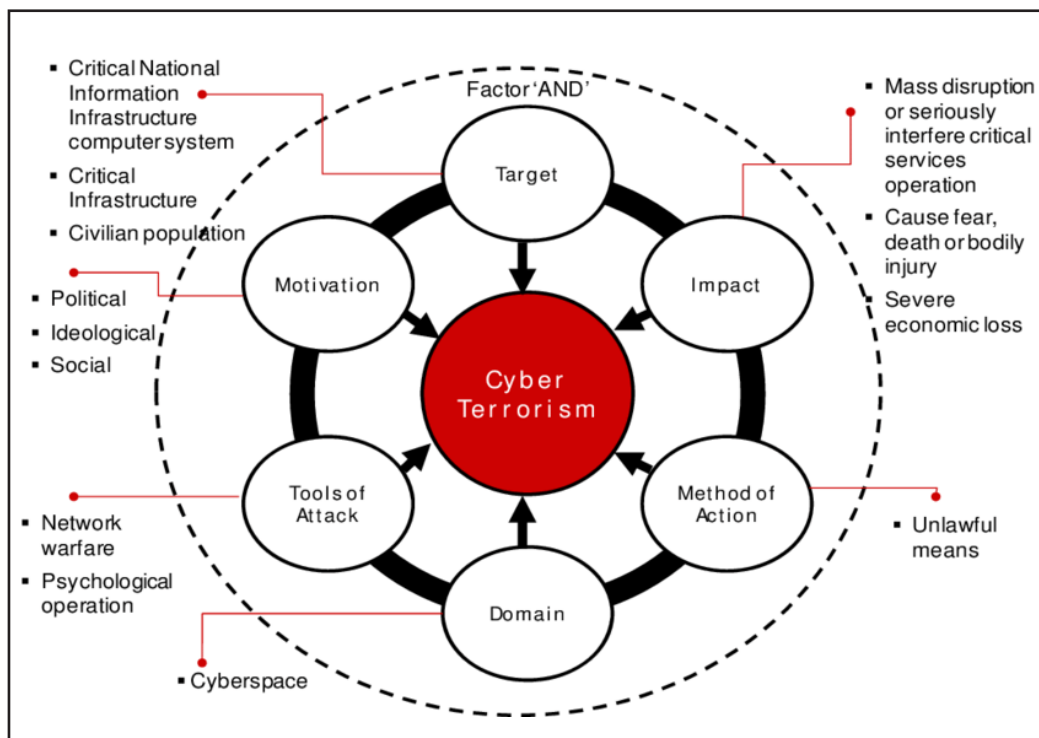
Cyber threats can be disaggregated, based on the perpetrators and their motives, into four:

- ❑ Cyber espionage: Intelligence gathering and data theft. The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization. Examples of this were Titan Rain and Moonlight Maze.

- Cyber crime: The use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.

	Cyber Espionage	Cyber Crime
Main Incentives	Information Gathering	Monetary gain, Vandalism
Targets	Few	Many
Malware Design	Tailored	Generic
Knowledge Required	Industry specific, IT security, Culture and language	IT security
Resources Required	Many	Few
Engineering Complexity	High	Low

- Cyber warfare: It involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks. Stuxnet is one of the best examples of cyber warfare in action.
- Cyber terrorism: It is premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence.



The Need for Cyber Security

- For Individuals: Photos, videos and other personal information shared by an individual on social networking sites can be inappropriately used by others, leading to serious and even life-threatening incidents.

- For Business Organizations: Companies have a lot of data and information on their systems. A cyber attack may lead to loss of competitive information (such as patents or original work), loss of employees/customers private data resulting into complete loss of public trust on the integrity of the organization.
- For Government: A local, state or central government maintains huge amount of confidential data related to country (geographical, military strategic assets etc.) and citizens. Unauthorized access to the data can lead to serious threats on a country.
- Various programs of government such as Aadhaar, MyGov, Government eMarket, DigiLocker, Bharat Net, etc. is prompting a larger number of citizens, companies and government agencies to transact online.
- India is the third largest hub for technology-driven startups in the world and its ICT sector is estimated to reach \$225 billion landmark by 2020.
- Increasing vulnerability: India the fifth-most vulnerable country in the world in terms of cyber security breaches. India saw at least one cybercrime every 10 minutes during the first half of 2017, including more sophisticated cyber threats, such as the WannaCry and Petya ransomware.
- Increasing internet users: India ranks 3rd in terms of the number of internet users after USA and China. By 2020, India is expected to have 730 million internet users with 75% of new users from rural areas.
- Increasing online transactions: For e.g., by 2020, 50% of travel transactions will be online, and 70% of e-commerce transactions will be via mobile.
- Government's digital push: Various programs of government such as Aadhaar, MyGov, Government e- Market, DigiLocker, Bharat Net etc. are prompting a larger number of citizens, companies and government agencies to transact online.
- Start-ups digital push: India is the third largest hub for technology-driven startups in the world and its ICT sector is estimated to reach \$225 billion landmark by 2020.
- India accounted for 5.09 per cent of all cyber attacks such as malware, spam and phishing attacks detected globally in 2017.
- Prevent economic loss: The estimated cost of cyber-attacks in India stands at four billion dollars which is expected to reach \$20 billion in the next 10 years.

Why India Needs a Digital Armed Force?

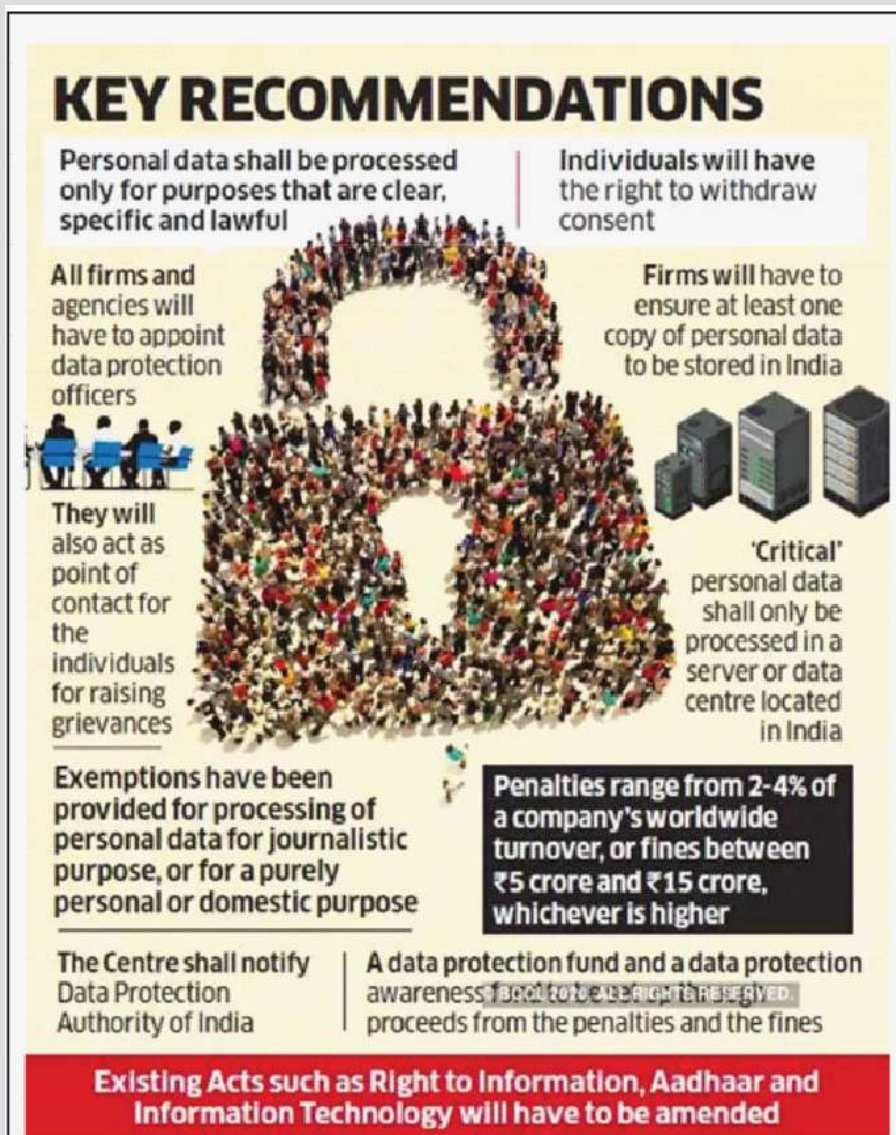
- To safeguard against Digital enemies, India needs to put in place a high-level Artificial Intelligence security system along with other digital security mechanisms to protect the digital borders.
- India is a prime target for several international spying agencies. Hence, we need to take the lead in indigenizing our entire IT infrastructure for national security.
- Digital enemies are very powerful and to safeguard our systems, we need to put in place a high-level Artificial Intelligence system along with other digital security mechanisms. We may be sitting at a time bomb and we must take every measure to defuse it.

Data Security

- Data security refers to the process of protecting data from unauthorized access and data corruption throughout its lifecycle. Data security includes data encryption, tokenization, and key management practices that protect data across all applications and platforms. According to Mukesh Ambani Data is the new oil.

Why Data Security?

- Organizations around the globe are investing heavily in information technology (IT) cyber defense capabilities to protect their critical assets. Whether an enterprise needs to protect a brand, intellectual capital, and customer information or provide controls for critical infrastructure, the means for incident detection and response to protecting organizational interests have three common elements: people, processes, and technology.
- Justice BN Srikrishna Committee report on need of data security
- A committee headed by retired Supreme Court Judge Justice BN Srikrishna submitted its report on "Data Protection Framework" to the Government.
- The Committee was constituted by the union government in July 2017, to deliberate on a data protection framework.
- The Supreme Court in its Puttaswamy judgment, 2017 declared privacy a fundamental right. This set the government in motion to take steps to bring a new data protection legislation for the country.
- The report has emphasized that interests of the citizens and the responsibilities of the state have to be protected, but not at the cost of trade and industry.
- The Committee has also proposed a draft Personal Data Protection Bill.



Challenges in Cyber Security

The general and universal challenges in cyber security are:

- ❑ Absence of any geographical barriers
- ❑ Attribution is very difficult as the attacker is difficult to locate
- ❑ Technology in cyberspace is rapidly evolving
- ❑ Traditional security concepts like deterrence and retaliation are difficult to apply
- ❑ Foolproof cyber security architecture is nearly impossible because of number of vulnerable points in the overall ecosystem

Challenges of Cyber Security in India

- ❑ Data colonization: India is a net exporter of information, however, data servers of majority of the digital service providers are located outside India. Also, data is being misused for influencing electoral outcomes, spread of radicalism, etc.
- ❑ Widespread digital illiteracy makes Indian citizens highly susceptible to cyber fraud, cyber theft, etc.
- ❑ Substandard devices: In India, majority of devices used to access internet have inadequate security infrastructure making them susceptible to malwares, such as recently detected 'Saposhi'. Also, rampant use of unlicensed software and underpaid licenses make them vulnerable as well.
- ❑ Lack of adoption of new technology: For eg, Banking infrastructure is not robust to cope-up with the rising digital crime as 75% of the total credit and debit cards are based on magnetic strip, which are easy to be cloned.
- ❑ Lack of uniform standards: There are variety of devices used with non-uniform standards which makes it difficult to provide for a uniform security protocol.
- ❑ Import dependence for majority of electronic devices from cellphones to equipments used in power sector, defense, banking, communication and other critical infrastructure put India into a vulnerable situation.
- ❑ Lack of adequate infrastructure and trained staff: There are currently around 30,000 cyber security vacancies in India but demand far outstrips supply of people with required skills.
- ❑ Under-reporting: majority of cases of cybercrime remains unreported because of lack of awareness.
- ❑ Lack of coordination among various agencies working for cyber security. Private sector, despite being a major stakeholder in the cyberspace, has not been involved proactively for the security of the same.
- ❑ Anonymity: Even advanced precision threats carried out by hackers is difficult to attribute to specific actors, state, or nonstate.
- ❑ Underreporting: More than 90% of cybercrime incidents remains under the sheet due to fear of reputational and credibility loss of an organization.
- ❑ Other challenges include absence of any geographical barriers, rapidly evolving technology in cyberspace and difficulty in establishing fool-proof cyber security architecture because of number of vulnerable points in the overall ecosystem.

Issues in India's cyber security strategy

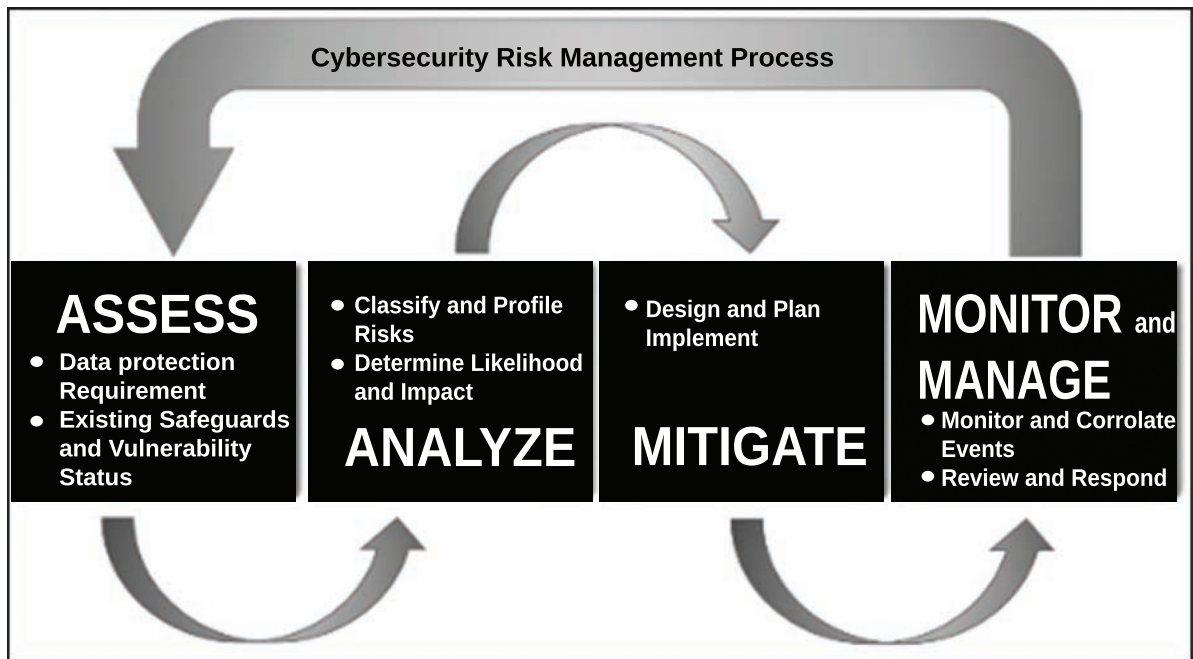
- ❑ Although the Government has set up the National Critical Information Infrastructure Protection Centre (NCIIPC) to protect the critical information infrastructure in the country; it is yet to identify and implement measures to protect "critical information infrastructure".
- ❑ The measure to appoint a National Cyber Security Coordinator in 2014 has not been supplemented by creating liaison officers in the States.

- Issues with National Cyber Security Coordinator-
 - ▶ It does not have any executive power since it is not under any Ministry.
 - ▶ It is not in the loop for cyber operations undertaken by the intelligence agencies.
 - ▶ Its faces lack of staff.
- Computer Emergency Response Team (CERT-In) is woefully understaffed.
- The private sector is equally culpable in its failure to report and respond to breaches in digital networks. Interpol data says that less than 10 per cent of such cases were registered with law enforcement agencies. Electronic fraud is notoriously underreported in India.
- There are neither voluntary, sector-specific standards for reporting data breaches nor industry backchannels for sharing confidential security information.
- Attitudinal factor - The continued perception has been that cyber security is “optional”. NIC email servers are often blamed for their poor security, but most Indian companies that rely on Gmail for official communication also do not make 2FA (two factor authentication) mandatory for its employees.
- International threat of a cyber-war from countries like China and Pakistan. Most of the cyber-attacks in India are done from Pakistan which are very carefully crafted. Those attacks that might affect the functionality of defence services are worrying for India like data acquisition systems.
- Rules of engagement on the Internet by governments and non-state actors are yet to be articulated.
- Lot of equipments in India are imported. It is unknown whether these devices are tampered with or programmed for control processes. Therefore, much more rigorous testing of the equipment that are being imported for telecommunication, power grid management or air traffic control should be done.
- Most of the cyber-attacks in India are done from Pakistan which are very carefully crafted. Those attacks that might affect the functionality of defence services are worrying for India like data acquisition systems.
- Still there is some ambiguity in responsibility of organisations for cyber security.
- Lack of Standards and Protocols- across the country in the cyber domain.
- Coordination in Public-Private Partnership- There is a serious mismatch of understanding between the civil sector and the government agency of cyber security.

Ways to prevent cyber attack

■ The steps to establish and maintain an adequate computer security programme are:

- Identify the computer system assets that require protection.
- Determine the value of each asset.
- Identify potential threats associated with each asset.
- Identify the vulnerability of the computer/EDP system to each of these threats.
- Assess the risk exposure for each asset.
- Select and implement security measures.
- Audit and refine the security programme on a regular basis.



❑ **A computer system security should include the following components:**

- Administrative and organizational security
- Personnel security
- Physical security
- Electronic security
- Hardware security
- Software security
- Operation security

❑ **The new technologies for preventing crimes are:**

- Firewall implemented with secure standards will not allow any intruder into the system.
- Encrypted tunneling: It allows secure communications across the internet. The data packets on the internet are encrypted, and then wrapped in IP at the initiation point of the tunnel. The encrypted packets can then be transmitted over the internet. When the packets arrive at the other end of the tunnel, they are unwrapped and decrypted.
- Crypto-currency mining: Crypto currencies can be mined using computational power, and profits can be earned as arbitrage between value of coins mined and the cost of infrastructure and power. Cybercriminals can exploit private and government infrastructure by deploying malware for mining crypto currencies in an unauthorised manner. From one compromised server in a data centre, a hacker can easily mine \$2,000 a month. This would cause loss of business, hardware damage and increased costs for the victims.
- Quantum computing: High-speed computers with tremendous computing power are being developed to assist artificial intelligence applications, robotics and machine learning. The computing power of these machines can easily break the current encryption technologies and cause havoc if they get into the hands of a cyber criminal.
- Secure Sockets Layer (SSL) and Secure HTTP (SHTTP) provides an encrypted TCP/IP. Pathways between two hosts on the internet (they require that both the browser and server be SSL-enabled). SSL can be used to encrypt any TCP/IP protocol (HTTP, FTP, and TELNET), SHTTP can only encrypt HTTP.

- Secure Electric Transform (SET) is the new technology for credit on internet. This involves cryptographic algorithms to encrypt the credit card numbers, so it cannot be seen on the internet.
- Digital signature: Cryptographic technique is used so that only authorized and authenticated person can enter in the system.
- Employee training to deal with cyber threats.

Gulshan Rai Committee recommendations on Cyber security:

- ▣ Establish a new Indian Cyber Crime Coordination Centre to check attempts of international gangs to penetrate Indian government official communication network.
- ▣ It would be linked to NATGRID and CCTNS (Crime and Criminal Tracking Network System) and branches in states to curb cybercrime.
- ▣ Devise an advance application for Social Media Analytics to monitor social media platforms activities related to Ministries of Home, External Affairs, Defence and other government organizations.
- ▣ Reduce Government's dependence on foreign servers and ensure one dedicated secure gateway for all government communication. A separate agency for online cybercrime registration, monitoring, and integration of CCTNS data with the same.
- ▣ Amend the Evidence act to suit the current requirements and prosecute the cybercrimes
- ▣ Sensitize the states by setting up cyber forensic laboratories in states along with workshops and international cooperation.
- ▣ CCTNS: aims to connect the police stations of the country to facilitate collection, storage, retrieval, analysis, transfer and sharing of data and information at the police station and between the police station and the State Headquarters and the Central Police Organizations.

Steps taken by Government India

▣ Cyber Security Strategy – India

- **Security Policy, Compliance and Assurance – Legal Framework**
 - IT Act, 2000
 - IT (Amendment) Bill, 2006 – Data Protection & Computer crimes
 - Best Practice ISO 27001
 - Security Assurance Framework- IT/ITES/BPO Companies
- **Security Incident – Early Warning & Response**
 - CERT-In National Cyber Alert System
 - Information Exchanges with international CERTs
- **Capacity Building**
 - Skill & Competence development
 - Training of law enforcement agencies and judicial officials in the collection and analysis of digital evidence
 - Training in the area of implementing information security in collaboration with Specialised Organisations in US
- **Setting up Digital Forensics Centres**
 - Domain Specific training – Cyber Forensics

- **Research and Development**
 - ▶ Network Monitoring
 - ▶ Biometric Authentication
 - ▶ Network Security
- **International Collaboration**
- **National Information Board (NIB):** National Information Board is an apex agency with representatives from relevant Departments and agencies that form part of the critical minimum information infrastructure in the country.
- **National Crisis Management Committee (NCMC):** The National Crisis Management Committee (NCMC) is an apex body of Government of India for dealing with major crisis incidents that have serious or national ramifications. It will also deal with national crisis arising out of focused cyber-attacks.
- **National Critical Information Infrastructure Protection Centre (NCIIPC):** Its purpose is to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders.
- **The National Cyber Coordination Centre (NCCC)** is an operational cybersecurity and e-surveillance agency in India. It is intended to screen communication metadata and co-ordinate the intelligence gathering activities of other agencies.
- **Cyber Dost:** the Ministry of Home Affairs runs a twitter handle called “Cyber Dost” that creates pertinent posts on prevention and protection against cybercrimes.
- India has already launched e-surveillance projects like National Intelligence Grid (NATGRID), Central Monitoring System (CMS), Internet Spy System Network and Traffic Analysis System (NETRA) of India, etc. None of them are governed by any Legal Framework and none of them are under Parliamentary Scrutiny. Thus, these projects are violate of Civil Liberties Protection in Cyberspace and provisions of
- National Informatics Centre (NIC) has been formed which provides network backbone Manages IT services, E -GOV initiatives to central and state governments.
- A new Cyber and Information Security (CIS) Division has been created to tackle internet crimes such as cyber threats, child pornography and online stalking.
 - ▶ Under this, Indian cyber- crime coordination centre (I4C) and Cyber Warrior Police force has also been established.
- Ministry of Defence formed Defence Cyber Agency in the realm of military cyber security.
- **Indian Computer Emergency Response Team (CERT-in) to enhance the security of India’s**
- Communications and Information Infrastructure through proactive action and effective collaboration.
 - ▶ **CERT-fin** has also been launched exclusively for financial sector.
 - ▶ **CERT-in** is also operating Cyber Swachhta Kendra, a Botnet Cleaning and Malware Analysis Centre.
- Government inaugurated the new body National Information Centre- Computer Emergency Response Team (NIC-CERT) to prevent and predict cyber-attacks on government utilities.
- The Ministry of Home Affairs is implementing the ‘Cyber-Crime Prevention against Women & Children’ Scheme.
- **Cyberdome Project:** Cyberdome is technological research and development Centre of Kerala Police Department.

- **Cyber Safe Initiative:** was launched by Maharashtra Government. The aim of the initiative is to spread awareness against atrocities committed against children and women. It will also create awareness about laws on cybercrime. The campaign is to be implemented all over the state by the State Government in collaboration with state police, public relations department and cyber cell.
- **Cyber Surakshit Bharat Initiative:** It was launched in 2018 with an aim to spread awareness about cybercrime and building capacity for safety measures for Chief Information Security Officers (CISOs) and frontline IT staff across all government departments.
- **Cyber Swachhta Kendra:** In 2017, this platform was introduced for internet users to clean their computers and devices by wiping out viruses and malware.
- Training of 1.14 Lakh persons through 52 institutions under the Information Security Education and Awareness Project (ISEA) – a project to raise awareness and to provide research, education and training in the field of Information Security.

Information Technology (IT) Act 2000

- Government of India enacted the Information Technology Act, 2000 (IT Act 2000) on 9th June, 2000 that provided a legal framework for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the government agencies.
- It was amended through Information Technology (Amendment) Act, 2008. This Act added provisions to the existing Information Technology Act, 2000 to deal with new forms of cyber-crimes like publicizing sexually explicit material in electronic form, video voyeurism, cyber terrorism, breach of confidentiality and leakage of data by intermediary, and e-commerce frauds.
- The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities which issues digital signature certificates for electronic authentication of users.
- The first and the only Cyber Appellate Tribunal in the country have been established by the Central Government in accordance with the provisions contained under Section 48(1) of the Information Technology Act, 2000.

Loopholes in IT Act:

- India does not have a dedicated cyber security law. The Information Technology Act, 2000, is not a cyber security law, which is why, breaches of cyber security continue to go unreported and there is no statutory elaboration of rights, duties, and responsibilities of stakeholders in this regard.
- A majority of cyber crimes are bailable offenses, which basically translates into inadequate deterrence to the offenders who violate the provisions of the law.
- The threat of data in the Cloud being lost: The Information Technology Act, 2000, has some provisions to deal with such cases of breaches of data on the Cloud, but they are only by way of compensation.
- Cyber criminals (often based outside the country) hack email accounts, websites and impose bogus profiles of celebrities across the web there’s no straight legal route to book them.
- There are no distinct dedicated cyber crime courts whose only job would be to deal with cyber crime matters for expeditious disposal of cases.

■ The National Cyber Security Policy of India 2013

- The National Cyber Security Policy of India 2013 (NCSP 2013) was announced by Indian Government in 2013. The policy aims to build a secure and resilient cyberspace for citizens, business and government.

- The mission of the policy is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

■ **Some of the shortcomings of the policy are:**

- The declared cyber security policy has proved to be a paper work alone with no actual implementation till date.
- The cyber security trends and developments in India 2013 have listed the shortcomings of Indian cyber security policy in general and Indian cyber security initiatives in particular.
- Indian cyber security policy has failed to protect civil liberties of Indians including privacy rights.
- Civil liberties protection in cyberspace has been blatantly ignored by Indian government and e-surveillance projects have been kept intact by the Narendra Modi government.
- The offensive and defensive cyber security capabilities of India are still missing.
- India is considered to be a sitting duck in cyberspace and cyber security field and the proposed cyber security policy has failed to change this position.

■ **Loopholes in the National Cyber Security Policy, 2013 (NCSP):**

- New technologies: The provisions to take care of security risks emanating due to use of new technologies e.g. Cloud Computing, has not been addressed.
- Use of social networking sites by criminals and anti-national elements: The policy does not address the issue.
- Missing tools to incorporate cyber crime tracking, cyber forensic capacity building and creation of a platform for sharing and analysis of information between public and private sectors on continuous basis.
- Creating a workforce of 500,000 professionals: There is no clarity whether this workforce will be trained to simply monitor the cyberspace or trained to acquire offensive as well as defensive cyber security skill sets.
- Safeguarding the privacy of citizen data: No specific strategy has been outlined to achieve this objective.

■ **The Personal Data Protection Bill 2019**

- The Personal Data Protection Bill 2019 (PDP Bill 2019) was tabled in the Parliament by the Minister of Electronics and Information Technology in 2019.
- The Bill covers mechanisms for protection of personal data and proposes the setting up of a Data Protection Authority of India for the same. Some key provisions the 2019 Bill provides for which the 2018 draft Bill did not such as that the central government can exempt any government agency from the Bill and the Right to Be Forgotten has been included.
- **The Bill aims to:**
 - ▶ to provide for protection of the privacy of individuals relating to their personal data,
 - ▶ specify the flow and usage of personal data,
 - ▶ create a relationship of trust between persons and entities processing the personal data,
 - ▶ protect the fundamental rights of individuals whose personal data are processed,
 - ▶ to create a framework for organisational and technical measures in processing of data,
 - ▶ laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data,

- ▶ remedies for unauthorised and harmful processing, and
- ▶ to establish a Data Protection Authority of India for the said purposes and for matters connected there with or incidental thereto.

National Cyber Exercise (NCX)

- The National Cyber Exercise aims to impart knowledge on current cyber threats, incident management, and response to top management and technical employees of government and critical sector businesses and organisations.
- Participants will learn about a variety of critical facets of cyber security, such as intrusion detection techniques, malware information sharing platforms (MISP), vulnerability handling and penetration testing, network protocols, and data flows, among others.
- The exercise will help strategic leaders better comprehend cyber threats, gauge their level of preparedness, and hone their collaboration and crisis management skills in the digital sphere.
- The National Security Council Secretariat (NSCS) coordinates the National Cyber Exchange (NCX) with cooperation from the Defense Research and Development Organization, the Data Security Council of India (DSCI), a knowledge partner (DRDO).

National Security Council (NSC):

The NSC is an executive government body entrusted with providing strategic and national security advice to the Prime Minister's Office. It has a three-tiered body structure. The Joint Intelligence Committee secretariat, the National Security Advisory Board, and the Strategic Policy Group make up the three echelons.

Indian Computer Emergency Response Team:

- The Indian Computer Emergency Response Team (CERT-In) has been chosen to represent the national organisation in charge of carrying out the following duties:
- Information gathering, analysis, and distribution regarding cyber events.
- Cyber security incident forecasts and warnings
- Emergency procedures for handling issues involving cyber security
- coordinating the response to cyber incidents
- To promote information security practises, processes, prevention, response, and reporting of cyber incidents, publish guidelines, advisories, vulnerability notes, and white papers.
- A vital part of India's cyber security against hackers and espionage as well as for monitoring terrorist activity online is the National Cyber Coordination Centre (NCCC).
- Digital India Surakshit: The Ministry of Electronics and Information Technology (MeitY) launched the Cyber Surakshit Bharat programme with the goal of developing a strong cyber-security ecosystem in India.
- ITU and India's joint cyber exercise: In order to teach Indian operators of vital network infrastructure, the Department of Telecommunications (DoT) and the International Telecommunication Union (ITU) launched the India-ITU Joint Cyberdrill event in December. Cyber security policy efforts in India and throughout the world were discussed by industry experts.

- ❑ When it comes to cyber security, India cannot afford to be complicit. An attack specifically targeted at these services might do far greater harm. India should modernise its infrastructure now rather than waiting for an attack.
- ❑ Particularly in the areas of power, transportation, and healthcare, the private sector has begun to play a substantial role in India's management of key information infrastructure.

International Measures

Budapest Convention on Cybercrime

- ❑ The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations.
- ❑ The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004. As of November 2018, 61 states have ratified the convention, while a further four states had signed the convention but not ratified it.

Why should India join?

- ❑ India would benefit from a proven framework under which nations commit to cooperate with each other to the widest extent possible with respect to cybercrime, and any crime involving electronic evidence.
- ❑ It can be the foundation for a global law on cyber security.
- ❑ It may help in guiding national legislation or policy against cybercrimes.
- ❑ It may ensure a collective action against using cyberspace to promote terrorist and extremist causes.
- ❑ India would become a priority country for capacity-building.
- ❑ India would be able to contribute to shaping future solutions if it were a party.

Arguments against joining are:

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

Paris Call

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

Significance of Paris Call

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

Internet Governance Forum (IGF)

- The IGF was established by the World Summit on the Information Society in 2006 to bring people together from various stakeholder groups in discussions on public policy issues relating to the Internet. While there is no negotiated outcome, the IGF informs and inspires those with policy making power in both the public and private sectors.
- The IGF facilitates a common understanding of how to maximise Internet opportunities and address risks and challenges. It is convened under the auspices of the Secretary-General of the United Nations.
- Its mandate includes the discussion of public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.

Council of Europe

The Council of Europe helps protect societies worldwide from the threat of cybercrime through the Budapest Convention on Cybercrime, the Cybercrime Convention Committee (T-CY) and the technical co-operation Programme on Cybercrime. The Budapest Convention on Cybercrime was adopted on 8 November 2001 as the first international treaty addressing crimes committed using or against network and information systems (computers). It entered into force on 1 July 2004.

ICANN

Internet Corporation for Assigned Names and Numbers (ICANN): It is a non-profit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. It has its headquarters in Los Angeles, U.S.A.

United Nations (UN)

- The International Telecommunication Union (ITU) is the specialized agency of the United Nations which is responsible for Information and Communication Technologies.

- ITU deals also with adopting international standards to ensure seamless global communications and interoperability for next generation networks; building confidence and security in the use of ICTs; emergency communications to develop early warning systems and to provide access to communications during and after disasters, etc.
- UN Secretary General formed panel on digital cooperation to tackle cyber security threats
 - United Nations (UN) has established first-of-its-kind panel on digital cooperation aimed at addressing concerns of cyber security threats and rise in hate speech. The high-level panel on digital cooperation will be co-chaired by US philanthropist Melinda Gates and China-based Alibaba founder Jack Ma.
 - The panel will have 20 members in total and include leaders from technology, public policy, science and academia etc. It will map trends in digital technologies, identify gaps and opportunities and outline proposals for strengthening international cooperation. It will focus on cyber-bullying, abuse rise, fake news, cyber crime and security aspects.

Way forward:

- India may consider acceding to Budapest convention.
- Prepare for cyber-attacks in various dimensions including space satellites.
- Implement a Cyber Crisis Management Plan.
- Cyber Security mock drills should be regularly conducted to prepare the organizations to detect, mitigate and prevent cyber incidence.
- The idea of a National Cyber Registry “as a repository of IT professionals” should be implemented.
- Currently, the only source of international guidelines on “cyber warfare” is the Tallinn Manual, a document that was put together by Western experts under the aegis of NATO.
- Concept of air gapping which isolate the critical infrastructures from the internet should be used.
- India must push for an international court to prosecute transnational cyber crimes, which would have the jurisdiction to try both state and non-state actors.
- The Indian government should promote attempts to create an international data protection law that facilitates quick information-sharing with multinational companies which do not host domestic servers.
- There is need to sensitize the people and institutions of cyber security measures, to make them report such attacks promptly, so that quick action can be taken.
- There is need to develop the offensive capabilities as well rather than being merely defensive.

Cyber Warfare

Cyber warfare involves units which are organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means. Hackers and other individuals trained in software programming and exploiting the intricacies of computer networks are the primary executors of these attacks.

Cyber-warfare involves the following attack methods:

- Sabotage: Military and financial computer systems are at risk for the disruption of normal operations and equipment, such as communications, fuel, power and transportation infrastructures.

- ❑ Espionage and/or security breaches: These illegal exploitation methods are used to disable networks, software, computers or the Internet to steal or acquire classified information from rival institutions or individuals for military, political or financial gain.

The Cyber-warfare has increased because:

- ❑ It is being considered as a legitimate mode of attrition between nations.
- ❑ With cyberspace all set to become the fifth dimension of warfare, countries around the world are busy preparing to face the threat of cyber war where attackers remain incognito.
- ❑ Anonymity is perhaps the biggest advantage associated with cyber-attack.
- ❑ A cyber weapon is an intellectual property (IP) which can be used in peace time and during war time. These weapons largely depend upon Zero Day exploits and vulnerabilities, and have limited shelf life.

Factors contributing/aggravating rise of Cyber-warfare

- ❑ The rapid evolution of threats, from non-state actors and at the behest or in some cases directly by state actors, has resulted in a global cyber pandemonium.
- ❑ The scenario has been further aggravated by the global incoherence of domestic and international cyber laws in relation to law enforcement model and most importantly non-availability of a global treaty, especially for issues relating to law of war model.
- ❑ At present, there are no formal rules of engagement in cyber warfare at either international or multi-lateral levels.
- ❑ Thus by all means, the stunning and crippling effect of cyber invasion could be a nightmare for security agencies and military establishments as cyberspace remains a “borderless and impersonal entity”. Clearly and apparently, cyber spies have no physical boundaries to negotiate while giving a practical shape to their “evil designs”.
- ❑ Satellites designed for communications, navigation, earth observation and many other end-uses could be paralysed and put out of commission through manipulation and degradation of their software. Hence a strong security system is needed to save the strategic infrastructure from cyber-attack.

Recent initiatives for tackling cyber warfare

- ❑ DRDO has been developing capabilities to produce robust high grade cryptographic devices based on indigenously developed cryptographic algorithms and indigenously architected high assurance platforms; and capabilities to develop advanced architectures for LAN and WAN security to safeguard information systems to counter external and internal threats has been developed. For the near term risk mitigation, DRDO works on the approach of development of software-based security systems running on COTS computing platforms.
- ❑ Government has signed Memorandum of Understandings between Indian Computer Emergency Response Team with Malaysia, Singapore and Japan. The MoUs related to Cyber Security will:
 - ❖ Promote closer cooperation for exchange of knowledge and experience in detection, resolution and prevention of security related incidents between India and respective country.
 - ❖ Each signatory country will share knowledge and experience in resolution, detection and prevention of security related incidents between India and the respective country.
- ❑ CERT-In is nodal department under the aegis of Union Ministry of Communications and Information Technology that deals with cyber security threats like hacking and phishing in India.

Pegasus Spyware

- The spyware Pegasus was created by the Israeli company NSO Group to assist spies in hacking into phones. The issue was brought to light in 2019 when Whatsapp sued the business in a US court.
- Hundreds of people, including Indians, were tracked via malware, according to a study published in July 2021 by Amnesty International and 13 international media sites.
- Despite NSO's assertion that their spyware is solely supplied to governments, no countries have so far offered to comply with these demands.

Concern related to Pegasus:

- Privacy violation: Whether or not a surveillance system is authorised by law, it violates both the right to privacy under Article 21 and the right to free expression under Article 19.
- Limiting dissenters: This trend of using hacking software against opponents and dissidents is concerning. Pegasus software was also employed in 2019 to hack Dalit and HR activists.
- Specific Security: Lack of privacy puts journalists' safety at risk, particularly those whose work criticises the government, as well as the safety of their sources.
- Self-censorship: A person may suffer from a constant fear of being watched. This may limit their capacity for such expression, acceptance, and discussion.
- Spyware combined with AI can tamper with digital content on users' smartphones, enabling state-sponsored mass surveillance. This may further divide people's opinions among remote controllers.
- National Security: If anything, advanced nuclear technology getting into the wrong hands would have worse repercussions than potential misuse or proliferation.

Chapter 6

ROLE OF MEDIA AND SOCIAL NETWORKING SITES IN INTERNAL SECURITY CHALLENGES

Role of media in internal security challenges

- In general, “media” refers to the tools of mass communication. Media today consists of television, Internet, cinema, newspapers, radio, magazines, direct mail, fax, and the telephone. Viewers can see some form of pictorial representation of messages through certain types of broadcasting and advertising. Images are visual representations, pictures, graphics, and include video, movies. Images are very useful in media to help get across messages effectively.
- Media constitute the fourth pillar of democracy. The role of the media is vital in generating a democratic culture that extends beyond the political system and becomes engrained in the public consciousness over time. Media is supplying the political information that voters base their decisions on. They identify problems in our society and serve as a medium for deliberation. They also serve as watchdogs that we rely on for uncovering errors and wrongdoings by those who have power. Media is vital in generating a democratic culture that extends beyond the political system and becomes engrained in the public consciousness over time. The role of media in a democracy is as crucial as that of the politicians and should never be underestimated.
- Media is the most powerful sector of an economy. It is a tool to maintain a balanced society which is characterized by well informed people, effective democracy and social justice. In fact, media has unparalleled influence on all aspects of human life in modern times. Basically, the media performs three functions to inform, to influence and to entertain. But effects of these functions are multidimensional in modern times. It has provided awareness about the whole world. In twenty-first century, media has a tendency to shape political, economical and social values of an individual.

Role of media in internal security

- Media role in internal security can be analyzed from the prism of news, views and issues. How it presents them to the populace can help either in strengthening or weakening of the basics of internal security. In the globalized world it has to strike a balance between people’s right to know on the one side and national security and social ethics on the other.
- If we look from the perspective of issues media can play a very important role in improving internal security as it plays the role of information provider, information disseminator. It can mould the perception of both people and government, can lead to re-formulation of policies if they are wrong and can prevent negative outcomes which could have arisen.

- ❑ Through its ground reporting it can warn of governments about the issues which can become security threat in future, like it can inform about the growing discontent in a particular area or group of people.

How has Indian media played its role in internal security?

❑ Positive role played by media

- Media in India has played its role very responsibly most of the times, but it also has its share of lapses.
- It has helped in bringing out the correct information regarding issues of naxalism, the ineffectiveness of the policies pursued and thus helping in course correction. It has fought tooth and nail against policies like that of SalwaJudum, which might have long term repercussions on national integration.
- It has highlighted the issues of displacement, inequitable growth, rising inequalities, forcible acquisition of land and other resources etc, which if not handled may become security threats in long term.
- Many a times it has brought out the reports of lapses in governments preparedness related to internal security and thus bringing accountability. In India media has played great role in highlighting the issues of human rights violation by security forces, absence of latest arms and technologies with police forces and thus creating a public opinion against such lapses.
- It has brought atrocities committed by security forces in light and course correction, which has helped in bringing people closer to governments as they feel that government care for them.
- It has helped in building resilience against any kind of efforts by ISIS to spread roots in India by creating a popular opinion against it.
- It has helped by giving a space for the dis-heartened people to vent their anger. This alternative has helped in maintenance of law and order in great way.

❑ Negative role played by media

- In terrorism: TV has been the most important broadcast media with reach comparable to newspapers. With the coming of cable TV in India, there has been a tremendous increase in the news channels available to an individual. Though news through print media comes only a day later, news channels via the broadcast media provide information 24x7. This enables them to provide real time information to the public especially those affected by the terrorist attack. But without any curbs on the amount of coverage, these forms of media can be used by the terrorists to mislead the investigation agencies and/or the public as was the case during the 26/11 Mumbai attacks. In the 26/11 attack, the handlers of the terrorist used the media coverage to tell them the exact locations of the policemen and advised them about the best way to attack the police. Thus the thoughtless media coverage, in a way helped the terrorist. Also the goriest details of the attack were shown virtually non-stop. Situations like the Mumbai attack check the credibility of our media. This incident certainly weakened the media demand to regulate itself.
- In Communalism: Broadcast media particularly news TV channels is often criticized for its non-stop live coverage of these incidents which might incite the communities to further wreak havoc. Even print media sometimes thoughtlessly carries messages from the leaders of opposing factions creating further tensions. One particular incident would be the Gujarat riots of 2002. The report of 'The Editor's Guild of India' on media ethics states that the local newspaper of Gujarat Sandesh had headlines which would "provoke, communalize and terrorize people. The newspaper also used a quote from a VHP leader as a headline, "Avenge with blood". But the same report also lauded some other local newspapers for their coverage. Broadcast media was heavily criticized for the gory images that were shown non-stop.

- In Cyber Space: The media networks are regularly hacked by enemy countries to spread false information and to recover classified data. Recently hacking of New York Times and Twitter servers by Syrian agencies was in news. Similarly the US and China continue to exchange blows in the field of hacking.

■ Other negative role played by media

- In recent times because of proliferation of news channels and rivalry with another for TRP instances of yellow journalism, dissemination of unverified news and one sided information by some unscrupulous news channels have emerged. Such actions of media have negative impact on long term internal security.
- The instances of playing too much with divisive issues, blowing news out of context have also surfaced in recent times. Seeking opinion of irresponsible individuals on sensitive issues may disrupt the social fabric of the country. This has also been aggravated by spread of social media which is taking the shape of public sourced media and also as a barometer of acceptance & popularity. This has made media houses dump objective reporting and playing to the tunes of masses who don't have knowledge of long term ill-effects of such things.
- Bomb blasts have taken place near the Delhi High Court, in Mumbai, Bangalore and so on. Within a few hours of such a bomb blast, many TV channels started showing news items that said that the Indian Mujahideen or the Jaish-e-Mohammed or the Harkatul-Jihad-e-Islam had sent e-mails or text messages claiming responsibility. The names of such alleged organisations will always be Muslim ones. Now, an e-mail can be sent by any mischievous person, but by showing this on TV channels and the next day in the newspapers, the tendency is to brand all Muslims as terrorists and bomb-throwers.
- The truth is that 99 per cent of the people of all communities, whether Hindu, Muslim, Christian or Sikh, and of whatever caste or region, are good. But the manner in which such news is shown on TV screens and published in newspapers tends to create the impression that all Muslims are terrorists, and evil — which is totally false. The person who sends such e-mails or text messages obviously wants to create hatred between Hindus and Muslims, which is the old British divide-and-rule policy continuing even today.
- Media does not have a wider perspective of India's national security issues.
- They generally do not apply brakes or observe self-restraint on its wayward and insensitive treatment of national security issues.
- Media's (especially electronic media) analysis and over-analysis of national security issues by groups of former diplomats, generals and academia's arm chair strategists distort national security perspectives.
- TV anchors discussing national security issues do not have much political and strategic maturity to discuss national security issues as their Western counter-parts do.

What should be done?

- Media is an important tool of statecraft and 'fourth pillar' of democracy. Our constitution ensures freedom of speech and expression which also includes freedom of press. But, it should be kept in mind that, this freedom must be exercised responsibly otherwise it can turn into a tool for creating disorder, confusion and mistrust. This in turn will bring media regulation by government in future, which will weaken the fourth pillar and democracy itself. The reasonable restrictions on freedom of speech must be treated as sacrosanct by media houses and must be self-adhered.
- There are two ways to remove these defects in the media. One is the democratic way, that is, through discussions, consultations and persuasion. The other way is by using harsh measures against the media, for example, by imposing heavy fines on defaulters, stopping government advertisements to them, suspending their licences, and so on.

- ❑ The media houses must evolve their own code of ethics and self regulation mechanisms through which actions against those acting against the interest of the national security can be taken.
- ❑ Governments must also be proactive and must continuously provide immediate, accurate and reliable information so that public is not influenced by sensational and biased news reporting.
- ❑ Media houses must also strengthen their local networks so that they can provide actual ground reports, can provide information in local languages because at present there exist a gap between local and national news which should be bridged.
- ❑ With emergence of multiple sources of information the credibility of information is lost. This aspect must be taken care of because credibility is of paramount importance for media.

Role of social media in internal security challenges

- ❑ Social media refers to internet-based communication among people who create, share and exchange their ideas, photos, videos and information on virtual cyber platform. It includes facebook, Twitter, YouTube, blogs, new micro blogging sites, etc. Its reach and popularity among people has rapidly increased over the last few years, primarily due to a sharp rise in the number of internet users and cell phone users. It is claimed that people spent more than 20% of the time spent on internet and on social media. Nearly 20 crore people use the internet in India. People freely exercise their right to express on social media as well as they get access to faster information and knowledge. Knowledge is power. Information is power. The variety of stand-alone and built-in social media services currently available introduces challenges of definition; however, there are some common features:
- ❑ Social media are interactive Web 2.0 Internet-based applications.
- ❑ User-generated content, such as text posts or comments, digital photos or videos, and data generated through all online interactions, is the lifeblood of social media.
- ❑ Users create service-specific profiles for the website or app that are designed and maintained by the social media organization.
- ❑ Social media facilitate the development of online social networks by connecting a user's profile with those of other individuals or groups.
- ❑ Users usually access social media services via web-based technologies on desktops and laptops, or download services that offer social media functionality to their mobile devices (e.g., smart phones and tablets). As users engage with these electronic services, they create highly interactive platforms through which individuals, communities, and organizations can share, co-create, discuss, participate and modify user-generated content or pre-made content posted online.

Challenges in adapting social media into policing are:

- ❑ Lack of clarity on how to use the technology
- ❑ Absence of adequate internet infrastructure
- ❑ Lack of immediate availability of talent
- ❑ Shortage of personnel and soft skills required to deal with a medium like social media at local levels
- ❑ Multiplicity of languages in India require further customization of technology which, in turn, requires Investment, both human and capital as well as redrawing of budget plans.

Threats due to Social Media

- ❑ **Cyber Terrorism:** The biggest challenge for internal security of nation through social networking site is cyber terrorism. Today terrorists select Social Media as a practical alternative to disturb the function of nations and other business activities because this technique has potential to cause huge damage. It poses enormous threat in international system and attracts the mass media, the security community, and the information technology corporation.
- ❑ **Fraud:** As Internet is growing explosively, online criminals try to present fraudulent plans in many ways.
- ❑ **Criminal Activity and Money laundering:** Internet Media is a major resource for developing serious crime. As Internet is growing explosively, online criminals try to present fraudulent plans in many ways. Social networking sites also pose major challenge in financial and organized crime which destabilizes the system. It creates threat to a company's security because of what employees might disclose and they are on prime target for cyber criminals.
- ❑ **International users:** The other national and international users such as the political parties, NGO's, hackers pose a serious threat using the social media. For example, during the civil turmoil in the Arab Spring Uprising, the various governments were threatened through the social media.
- ❑ **To Bring Revolution:** Some countries in the world feel threatened by the fact that social media can bring the people together and thus, create a revolution. This in turn can cause political instability.
- ❑ **Communal Violence and Fanning Tensions:** Importantly, social media also seems to be playing a significant role in polarising different communities in India and compounding India's Security challenges. The viral videos and false updates of communal clashes, riots and terrorists attack have created a massive impact in the life of public.
- ❑ **Virtual Community:** Popular social networking websites are another means of attracting potential members and followers. These types of virtual communities are growing increasingly popular all over the world, especially among younger demographics. This can build Anti-national Sentiments among Society.
- ❑ **Hacking:** Hackers write or use ready-made computer programs to attack the target computer. By using Social Media hackers breach the national security and steal important data of defence or other strategic sectors. This can kneel the whole country without using Arms and Ammunition.
- ❑ **Fake news:** The social media enable each user to be a news broadcaster. As a result the vested interests are using social media to spread fake news. This fake news can cause threat to peace and stability of the society.

Challenges in Monitoring Social Media

- ❑ **Server Location and Laws of Different Countries:** Lack of Geographical Boundaries makes social media regulation an arduous task. Major Complicating Factors to secure the networks and Media Much of the hardware and software that make up the communications ecosystem is sourced externally.
- ❑ **Encrypted Message:** Use of phones/whatsapp to send and receive messages, concerns the government because the communications sent via such devices and applications are encrypted and could not be monitored and consequently hinders the country's efforts to fight terrorism and crime.
- ❑ **Complicated 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 who see measures such as security auditing and other regulations and frameworks as adding to their costs. Source of Origin is difficult to find out.
- ❑ **Accountability issues:** Challenges with respect to fixing the liability of intermediaries in cases like forwarded messages on social media platforms like WhatsApp, Facebook, etc.

- ❑ Anonymity: Police officers have expressed concern over multiplicity of fake profiles that make it even more difficult to track the offenders.
- ❑ Legal challenges such as Internet traffic monitoring and privacy Concerns, fears of censorship and threat to freedom of speech and expression.

Regulation of Social Media in India for Internal Security

❑ Legislative Regulation:

- Information Technology Act, 2000
- Indian Penal Code
- The Evidence Act, 1872
- Banker's Book Evidence Act, 1891

Many electronic crimes do on Social media have been bought within the definition of traditional crimes by means of Amendment to the Indian Penal Code, 1860. The Evidence Act, 1872 and the Banker's Book Evidence Act, 1891, too, have been suitably amended in order to facilitate collection of evidence in fighting electronic crimes. These laws also stipulate the liability of various stakeholders in the social media ecosystem, specifically in the context of access of social media through mobile devices.

❑ Surveillance Projects in India

- e-Surveillance Projects: National Intelligence Grid (NATGRID), Central Monitoring System (CMS), Internet Spy System, Network and Traffic Analysis System (NETRA) of India, National Critical Information Infrastructure Protection Centre (NCIPC) of India, National Cyber Coordination Centre (NCCC) of India, Tri-Service Cyber Command for Armed Forces of India, Cyber Attacks Crisis Management Plan Of India.

❑ Recent steps taken by Ministry of Home Affairs for monitoring social media:

- Union home ministry has decided to constitute a panel to monitor cybercrimes and ensure compliance of complaints by social media platforms.
- It is sensitising law enforcement agencies to enhance coordination with the Department of Telecom, which is the nodal body to flag violation of IT Act with social media platforms.
- MHA held meeting with representatives of social media platforms such as Google, Facebook and Twitter to discuss measures required to filter malicious content such as hate speech and video linked to terror, child pornography and fake news from appearing on social media.

Ways to address the challenge of social media

- ❑ Digital Education: The lack of digital literacy has led to people falling prey to social media manipulations and agenda of vested interests. Spreading of digital education can effectively prepare people to be aware of intricacies of social media and avoid falling prey to agenda of vested interests.
- ❑ Strengthening cyber intelligence: Cyber security ambit needs to be expanded to involve cyber intelligence. Utilising technologies like artificial intelligence and big data analytics government can counter internal security threats emanating from social media.
- ❑ Accountability on social media platforms: Social media platforms are benefitting from user traffic. They must be bestowed with responsibility for threats emanating from their platforms. This will nudge them from developing internal mechanisms to counter the threats.
- ❑ Smart policing: Policing systems need to update so that they can cater to the new age realities. Police need to be techsavvy so that they are aware of the threats emanating from the social media platforms.

- ❑ Mining Social Media for Intelligence: The government can effectively use social media for intelligence purpose.

Crypto-currency and National Security

- ❑ The growing use of cryptos has led to several innovations and changes in the global economic sphere. However, the anonymity of cryptos may become a serious threat to India's national security.

❑ About Crypto Currency:

- Crypto-currency is a decentralised, digital, encrypted form of currency. It is a sort of concealed, safe, and uncontrived digital or virtual currency. Everything is online, so it doesn't have a physical source.
- In a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" published in 2008, Satoshi Nakamoto first proposed the fundamentals of the first crypto-currency, Bitcoin.

❑ What distinguishes crypto-currencies from other online payment methods?

- The main difference between regular cash and crypto-currency is that with crypto-currency, payments may be made directly between two people without the need for a middleman bank.
- It's not necessary to link your money to a bank account. Banks or any other financial institutions are not in charge of regulating crypto-currency transactions.
- It is therefore recognised as one of the safest payment options. Block chain technology is a technique for keeping track of all of these crypto-currency transactions.

❑ Crypto Currency: Indian conundrum

- In India, there are between 15 and 20 million crypto-currency investors, with a total market cap of about 400 billion rupees (\$5.37 billion). The government of India declared in Budget 2022 that revenue from crypto-currency and other digital assets will be subject to a 30% tax.
- Many nations, including Saudi Arabia and Turkey, have outright outlawed crypto-currency. Other nations, including the USA, Japan, and Canada, have put sensible limitations in place.
- The Reserve Bank of India (RBI) will soon launch a digital currency backed by the central bank, according to government announcements made in the most recent budget (CBDC).

❑ How is crypto-currency a threat to national security?

- Terrorism (through the dark web): Militant organisations' use of crypto-currencies on the dark web for terror actions and drug trafficking is a serious danger to national security and a major issue for Indian security services.
- The most sophisticated means of financing terrorism have arisen as crypto-currencies, and when they are used on the dark web, such as TOR, Freenet, Zeronet, and Perfectdark, they are untraceable to security authorities.
- Money laundering: Because crypto-currencies like Bitcoin, Monero, Ripples, and Zcash offer anonymity and non-traceability, money launderers, cybercriminals, and terrorists find them very useful.
- According to the UN Vienna 1988 Convention, money laundering is the conversion of property obtained from any crimes in order to hide the source.
- Money laundering is defined by India's Prevention of Money Laundering Act, 2002 (PMLA), as an action related to the attempt to portray criminal proceeds as pristine property.
- Illegal game: This phenomenon does not have a regulated legal framework.

- Crypto scams: There are many different types of crypto currency frauds, which affect a wide spectrum of people. Scam Initial Coin Offerings, where con artists sell crypto currency coins to a select group of investors before disappearing after the sale.
- Pump and Dump schemes, where fraud is continued when a shady organisation first sells coins based on a show before selling entire holdings when the value increases.
- Examples of scams include the One Coin Scam, the Bit Connect fraud, the Karnataka Bitcoin scam, and the \$10.5 billion in fraud using Defi platforms that was reported in 2021.

Dark Net:

- The dark net is a hidden, fluctuating region of the internet where it is impossible to determine a user's identity since their identity is completely hidden by their router browser. Due to end-to-end encryption, it protects the user's identity when communicating with other users.
- Popular dark net browsers include the TOR software, Freenet, Zeronet, and Perfect Dark, which can only be accessed by specialised software.

Current laws:

- In India, crypto-currencies have been operating in an unregulated environment due to a lack of regulatory legislation. (The Supreme Court overturned an RBI Circular banning regulated organisations from transacting in virtual currency in 2020.)
- The PMLA serves as the main piece of legislation for AML and CFT, and it is supported by other pieces of legislation like the Foreign Exchange Management Act of 1999, the Securities and Exchange Board of India Act of 1992, the AML Guidelines from 2006, and an RBI Master Circular.
- By design, crypto currency ecosystems don't use established institutional middlemen, hence they might not be governed by the law at this time. Money laundering using crypto currency has so far mostly been established through statistical space.
- Despite the fact that the Enforcement Directorate has occasionally looked into the function of exchanges, neither crypto currency nor exchanges are considered entities for the purposes of the PMLA/FEMA. How the courts would handle any such criminal culpability within the purview of existing laws and regulations is yet to be determined.
- The Financial Action Task Force (FATF) has been making recommendations about virtual currencies on a global scale. Updated Guidance on Virtual Assets, published by the FATF in 2021, suggests that intermediaries be subject to particular activity-based AML/CFT duties as well as compliance and oversight measures.

Way forward:

- The Crypto-currency Bill is something the Indian government intends to introduce in Parliament. It seems unclear that the proposed legislation will put an end to the argument over whether to regulate crypto-currencies or completely outlaw them, even if the step has been long overdue.
- Crypto currencies should be regulated rather than outlawed, as suggested by protectionists who want to stop illegal activity, protect against volatility, and prevent speculation. This is because of the potential for job creation and GDP contribution to India.
- Less than 1% of illegal behaviour is conducted through crypto currency transactions, according to research, which is another factor supporting the case. The majority of that linked crime involving crypto currency is scams. Nevertheless, it is acknowledged that neither strategy alone would be sufficient to stop illegal activity carried out over P2P networks, which are by their very nature resistant to institutional control.

- The likelihood of illicit acts related to crypto currencies may be reduced by inclusive legislation with tight enforcement (via required KYC (know your customer), real-time suspicious transaction reporting, industry-wide compliance standards, strict reporting, and regulator monitoring).
- In contrast to a comprehensive ban, which may further push unlawful transactions underground and make it harder to trace them down and punish the honest investor, permitting economic growth and financial inclusion. As a starting step, a thorough crypto currency bill would go a long way toward creating a sound regulatory structure that is open to all participants in the ecosystem.

Chapter 7

ISSUES RELATED TO SECURITY FORCES

Central Armed Police Forces

- The Central Armed Police Forces (CAPF) refers to seven security forces in India under the authority of Ministry of Home Affairs. They are Assam Rifles (AR), Border Security Force (BSF), Central Industrial Security Force (CISF), Central Reserve Police Force (CRPF), Indo Tibetan Border Police (ITBP), National Security Guard (NSG), Sashastra Seema Bal (SSB). Each of the seven has its own cadre of officers, but they are headed by officers of the Indian Police Service.

Major bodies dealing with the Internal Security

■ Assam Rifles (AR)

- Known as 'Friends of the Hill People', Assam Rifles, raised initially as Cachar Levy in 1835, is the oldest Police Force in the country with headquarters at Shillong.
- The Force has a dual role of maintaining internal security in the North Eastern region and guarding the Indo- Myanmar Border.
- They perform many roles including the provision of internal security under the control of the army through the conduct of counter insurgency and border security operations, provision of aid to the civil power in times of emergency, and the provision of communications, medical assistance and education in remote areas.

■ Border Security Force (BSF)

- The Border Security Force (BSF) is the primary Border Guarding police force of India.
- It was raised in the wake of the 1965 War on 1 December 1965, "for ensuring the security of the borders of India and for matters connected there with".
- BSF was raised in 1965 and the multiplicity of State forces guarding the Indian borders with the neighbouring countries was done away with.
- Its operational responsibility is spread over 6385.36 kms. Of international border along Indo-Pakistan, Indo-Bangladesh borders.

- It currently stands as the world's largest border guarding force. BSF has been termed as the First Wall of Defence of Indian Territories.
- BSF is the only Central Armed Police force to have its own Air Wing, Marine Wing and artillery regiments, which support the General Duty Battalions in their operations.

■ Central Reserve Police Force (CRPF)

- Initially raised as Crown Representative Police on July 27, 1939 at Neemuch (MP), the Force was rechristened as Central Reserve Police Force (CRPF) after Independence.
- The Force is presently handling a wide range of duties covering law and order, counter insurgency, anti-militancy and anti terrorism operations.
- The Force plays a key role in assisting States in maintaining public order and countering subversive activities of militant groups.
- The Central Reserve Police Force is the largest of India's Central Armed Police Forces. It is also operating abroad as part of United Nations peacekeeping missions.

■ Central Industrial Security Force (CISF)

- Raised in the year 1969, CISF is presently providing security cover to important installations like space and atomic energy establishments, sea ports, airports, coal mines, steel plants, thermal and hydel power plants, oil and petrochemicals installations, heavy industries, defence establishments, security presses, museums and historical monuments.
- The specialized task of airport security was assigned to CISF in the wake of hijacking of Indian Airlines plane to Kandhar.
- The charter of CISF has been expanded to provide security cover to VIPs as well as to provide technical consultancy services relating to security and fire protection to industries in public and private sectors.

■ Indo-Tibetan Border Police (ITBP)

- Indo-Tibetan Border Police Force was raised in the wake of India China conflict in 1962.
- ITBP is a mountain trained Force. Forces are called "Himveer".
- It is deployed from the north-western extremity of the Indo-China Border upto the tri-junction of India, China & Nepal covering mountainous terrains.
- Presently, battalions of ITBP are deployed on border guard duties from Karakoram Pass in Ladakh to Diphu La in Arunachal Pradesh, on the India-China border.
- ITBP is in the forefront of movement for the preservation of Himalayan environment & ecology.

■ Sashastra Seema Bal (SSB)

- Special Service Bureau (SSB) was set up in the early 1963 in the wake of India China conflict of 1962 to build people's morale and inculcate spirit of resistance in the border population against threats of subversion, infiltration and sabotage from across the border.
- As a border guarding force and lead intelligence agency (LIA) for Indo-Nepal border and Indo-Bhutan border.
- To prevent trans-border crimes and unauthorized entries into or exit from the territory of India.
- To prevent smuggling and other illegal activities.

■ National Security Guard (NSG)

- National Security Guard was raised in 1984, following Operation Blue Star and the assassination of Indira Gandhi, "for combating terrorist activities with a view to protect States against internal disturbances"

- It has been modelled on the pattern of SAS of the UK and GSG-9 of Germany.
- The NSG's is trained to conduct counter terrorist task to including counter hijacking tasks on land, sea, and air; Bomb disposal and Hostage Rescue missions.
- The primary role of this Force is to combat terrorism in whatever form it may assume in areas where activity of terrorists assumes serious proportions, and the State Police and other Central Police Forces cannot cope up with the situation.

■ Other forces/institutions

- National Disaster Response Force (NDRF)
- Home Guards
- The National Foundation for Communal Harmony
- National Investigative Agencies (NIA)
- Bureau of Police Research & Development (BPR&D)
- National Crime Records Bureau (NCRB)
- Narcotics Control Bureau (NCB)
- Directorate of Revenue Intelligence (DRI)
- Central Bureau of Investigation (CBI)
- Intelligence Bureau (IB)
- Research and Analysis Wing (RAW)

Issues with Paramilitary Forces

- The paramilitary forces personnel were grieved by the non-grant of “equal pay for equal work”; a benefit granted to the organised defence services.
- The paramilitary forces officers are not being given special allowances on the lines of defence forces even though they work in tougher conditions and round the clock.
- The paramilitary forces are engaged throughout the year in duties like elections, crowd control, rescue operations, VIP arrangements and other internal security managements.
- The paramilitary forces are still been placed in the ‘civil’ category even though their work profile ranges from guarding the border, managing tense situations, fighting the naxals and insurgent groups in different areas on the tough terrains.
- Officers of the three defence forces – Army, IAF and Navy – are paid 29% higher salary compared to their civilian counterparts from the IAS, IPS and other ‘Group A’ Services at the starting level.
- Recently about 60 per cent of the officers selected for posting in the Border Security Force (BSF) have refused to join, citing reasons for second class treatment meted out to paramilitary forces as compared to the armed forces and stagnation of career.

Suggestions

- Suggestions have often been given to the home ministry to bring about some kind of rotation in the duties of these personnel, so they have time to refresh themselves and recuperate.
- However, these ideas did not find favour. No wonder there is considerable attrition within the forces and large numbers go on voluntary retirement after completing the mandatory 20 years of service.
- The existing grievance redressal mechanism needs to be revisited. It will have to be made more broad-based. More channels need to be opened for grievances to be aired.

- ❑ The government of India would be well advised to set up a high-powered commission to look into the plethora of problems facing the Central Armed Police Forces and suggest long-term solutions for those.
- ❑ Government has notified 7th Pay Commission for the military. It has approved increment in the pay matrix from 24 to 40 years.

Police Reforms

Under the Constitution, police is a subject governed by states. Therefore, each of the states has their own police forces. The centre is also allowed to maintain its own police forces to assist the states with ensuring law and order. Therefore, it maintains seven central police forces and some other police organisations for specialised tasks such as intelligence gathering, investigation, research and record-keeping, and training. The primary role of police forces is to uphold and enforce laws, investigate crimes and ensure security for people in the country. In a large and populous country like India, police forces need to be well-equipped, in terms of personnel, weaponry, forensic, communication and transport support, to perform their role well.

Issues in Police Reforms

- ❑ Political authorities have a stronghold over police this nexus affects the credibility of the police too.
- ❑ Most of the times the State Police Training Schools where a large majority of policemen undergo training are ill equipped, starved of funds and staffed by unwilling instructors.
- ❑ NHRC has made it very clear that “with every passing year, the evidence before the Commission mounts that there must be major police reforms in the country if the human rights situation is to be improved”.
- ❑ It is general observation that the intelligence gathering efforts are devoted mainly to gathering information about major law and order problems, while adequate attention is not paid to collection of intelligence relating to commission of crimes.
- ❑ Since the police is the primary agency of the criminal justice system which protects human rights, it is essential to sensitise police personnel to gender issues.
- ❑ Gender disparity is another issue as in the criminal justice system; the representation of women is low in all wings and especially the police.

Major suggestions in Police Reforms

- ❑ Increase budget expenditure on police.
- ❑ Improving police infrastructure.
- ❑ Independent Complaints Authority.
- ❑ Need to adopt latest IT- enabled services.
- ❑ Improve Citizen police participation like bhagidari in delhi and janamaitri suraksha in kerala
- ❑ Police should be made more gender sensitive. 33% women reservation in police should be implemented
- ❑ There is need for broader political awareness about the need for police reform. Some states like Kerala and Telangana have tried to take the process forward.
- ❑ Need to strengthen Criminal Justice System and grassroots level policing institutions.
- ❑ Strengthen its investigative capabilities and emergency response infrastructure.
- ❑ More investment is needed in the recruitment procedure.
- ❑ Better training, better pay and allowances and creating a system that rewards initiatives need to be incorporate.

Police Reform with Respect to Cyber Security

Cyber Security is protecting cyber space including critical information infrastructure from attack, damage, misuse and economic espionage. Cyber Security is “the security of information and its communicating channels as applied to computing devices such as computers and smart phones, as well as computer networks such as private and public networks, including the Internet as a whole.” The cyber security threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, security of nation and the stability of the globally linked economy as a whole. The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain and the act can take place from virtually anywhere. These attributes facilitate the use of Information Technology for disruptive activities. As such, cyber security threats pose one of the most serious economic and national security challenges.

Major Examples of cyber crimes

- ❑ Through a phishing email sent to an employee, hackers accessed the credentials to execute a fund transfer, swindling Union Bank of India of \$171 million; Prompt action helped the bank recover almost the entire money.
- ❑ The global ransom ware attack took its toll in India with several thousand computers getting locked down by ransom-seeking hackers. The attack also impacted systems belonging to the Andhra Pradesh police and state utilities of West Bengal.
- ❑ The food tech company Zomato discovered that data, including names, email IDs and hashed passwords, of 17 million users was stolen by an ‘ethical’ hacker-who demanded the company must acknowledge its security vulnerabilities-and put up for sale on the Dark Web.
- ❑ Petya ransomware attack made its impact felt across the world, including India, where container handling functions at a terminal operated by the Danish firm AP Moller-Maersk at Mumbai’s Jawaharlal Nehru Port Trust got affected.

Issues with Cyber Security

- ❑ Cyberspace has inherent vulnerabilities that cannot be removed.
- ❑ Internet technology makes it relatively easy to misdirect attribution to other parties.
- ❑ It is generally seen that attack technology outpaces defence technology.
- ❑ Lack of awareness on Cyber security.
- ❑ Lack of Cyber security specialists.
- ❑ Increased use of cyberspace by terrorists.
- ❑ Photos, videos and other personal information shared by an individual on social networking sites can be inappropriately used by others, leading to serious and even life-threatening incidents.
- ❑ Companies have a lot of data and information on their systems. A cyber attack may lead to loss of competitive information (such as patents or original work), loss of employees/customers private data resulting into complete loss of public trust on the integrity of the organization.
- ❑ A local, state or central government maintains huge amount of confidential data related to country (geographical, military strategic assets etc.) and citizens. Unauthorized access to the data can lead to serious threats on a country.
- ❑ Increased use of mobile technology and internet by people.
- ❑ Proliferation of Internet of Things (IoT) and lack of proper security infrastructure in some devices.

Suggestions related to Cyber Security

- ❑ Using Artificial Intelligence (AI) for predicting and accurately identifying attacks.
- ❑ Using the knowledge gained from actual attacks that have already taken place in building effective and pragmatic defence.
- ❑ Increased awareness about cyber threats for which digital literacy is required first.
- ❑ India needs to secure its computing environment and IoT with current tools, patches, updates and best known methods in a timely manner.
- ❑ The need of the hour for Indian government is to develop core skills in cyber security, data integrity and data security fields while also setting stringent cyber security standards to protect banks and financial institutions.
- ❑ Real-time intelligence is required for preventing and containing cyber attacks.
- ❑ Periodical 'Backup of Data' is a solution to ransom ware.

Need for reforms in the country's Intelligence Apparatus

There are five components of national security management, namely (i) diplomacy, (ii) economy, (iii) military, (iv) internal security, and (v) intelligence. Intelligence service is defined as the collection, collation, analysis and assessment of information pertaining to national security or having a bearing on formulation of national strategies

India's Intelligence apparatus

- ❑ India's intelligence apparatus consists of various agencies, of which the Intelligence Bureau (IB) is the oldest. IB reports to the Ministry of Home Affairs and is responsible for India's domestic intelligence, internal security, and counter-intelligence.
- ❑ The Research and Analysis Wing (R&AW), meanwhile, is the country's foreign intelligence agency.
- ❑ The National Technical Research Organisation (NTRO), is the technical intelligence agency of the Government of India.
- ❑ There is also the Directorate of Revenue Intelligence (DRI) that is tasked with anti-smuggling intelligence

New Challenges of national security management:

- ❑ **There are Conventional threats like**
 - offensive armed postures by hostile powers,
 - Nuclear, biological and chemical threats,
 - Terrorism and insurgency
 - Transnational crimes (e.g. drug smuggling or trade in counterfeit currency)
 - Human trafficking

■ **Non-conventional and newer challenges include:**

- Migration
- Epidemics (Like the ongoing COVID pandemic)
- Natural disaster
- Environmental security
- Cyber terrorism

■ **Challenges faced by intelligence agencies:**

- Ambiguity in the functioning and overlap in functioning : Like Defence Intelligence Agency (DIA) and NTRO have overlapping role in collecting technical and communications intelligence.
- Ad-hoc decision making: Many of its intelligence agencies are created not as part of a deliberate strategic vision, but merely as a response to a crisis, like R&AW was created in response to the Kargil war.
- Inadequate intelligence: Like intelligence failure in Sino-India confrontation on LAC, in May 2020.
- Lack of dedicated cadre: The different branches of the military have their own intelligence wings and have their own cadre of intelligence officers. The same problem lies with the civilian intelligence systems.
- Lack of insight for the newer threats : New threats like Pegasus malware attack managed to breach the WhatsApp communication platform's end-to-end encryption protocol
- Need for better accountability and oversight.

Suggestions for reforms:

- Introduce legislation in Parliament for laying down the charters, functions and duties of intelligence organisations and provide a legal basis for different tiers of accountability.
- Have open and separate direct recruitment mechanisms for different intelligence agencies
- Improve training for analysts in tools of modern prescriptive work
- Enhance in-house technical research and development capabilities especially in relation to signals decryption work, and cryptography capabilities
- Upgrade offensive as well as defensive capabilities in cyber warfare
- Introduce a system of interchangeability between various intelligence agencies and the connected Ministries of the Government of India.
- Appoint a National Intelligence Coordinator/Director of National Intelligence to bring about better interagency coordination, remove overlaps and duplications, end 'turf-wars' and ensure better utilisation of national resources
- Set up a Parliamentary Accountability Committee for oversight of intelligence agencies through legislation

Conclusion

Given the immense new security challenges confronting India as it emerges as a global power, a paradigm shift is needed to modernise intelligence work in a holistic manner, which may require radical changes in the existing intelligence culture. The Indian intelligence community has for too long fallen short of expectations and now is the time to remedy the lacunae.

Coastal Security

India's 7,516-kilometre-long coastline includes 5,422 kilometres of coastline on the mainland and 2,094 kilometres on the islands belonging to nine states and four Union Territories. The coastline accounts for 90% of the country's trade and it spans 3,331 coastal villages and 1,382 islands. The coastline houses 12 major and 200 minor ports, along with 95 landing centres, and is increasingly facing security challenges from adversarial neighbours and non-state actors. This has necessitated the adoption of a more structured and holistic approach with a long-term strategy to modernise, update and strengthen naval surveillance and to plug loopholes in coastal security architecture.

Issues with Coastal Security

- ❑ Difficult terrain, seasonal weather patterns, administrative lapses, etc. all contribute towards introducing gaps in surveillance and the monitoring mechanism.
- ❑ Delays in land acquisition and support infrastructure, such as barracks and staff quarters at several locations.
- ❑ Low infrastructure creation (only 31%): Jetties under the Coastal Security Scheme were yet to be constructed. Use of fisheries' piers by coastal police at extended distances from Coastal Police Stations (CSS)
- ❑ Below par state-level monitoring mechanisms.
- ❑ The involvement of different agencies and ministries at centre, state and local level invariably leads to coordination problems although several efforts have been made to create greater synergies between them.
- ❑ Lack of clarity among various stakeholders about their roles in ensuring coastal security.
- ❑ Acute shortage of manpower in police stations, (only 25% of the sanction)
- ❑ Poor Training: Lack of a dedicated training academy for the ICG.
- ❑ Discontent in fishermen communities interferes with the effective functioning of the coastal security architecture as fishermen are considered the 'eyes and ears' of the coastal security architecture and, therefore, an integral part of it.

Suggestions for Coastal Security

- ❑ Capacity building of the maritime police force both in terms of training as well as resources should be done at par with other maritime security agencies like Navy and Coast Guard.
- ❑ Up gradation of coastal security infrastructure with latest equipments and gadgets.
- ❑ The government is considering doing away with state maritime police forces that are in place in the nine coastal states and four union territories.
- ❑ There is a proposal that the Coast Guard, which comes under the Defence Ministry's jurisdiction, will now be placed under the Union Home Ministry and designated as the National Maritime Police (NMP).
- ❑ Regular coastal security exercises like Sea Vigil, bi-annual Sagar Kavach, should be conducted to audit the actual security scenario.
- ❑ The potential threat from smaller rogue boats is likely to be addressed through a satellite-guided friend or foe identification system of the Indian Space Research Organisation with a two-way messaging system in all local languages.
- ❑ Enlist sailors who are about to retire, to man the state maritime police forces.
- ❑ Fishermen and coastal communities should be included in the comprehensive coastal security plan as 'eyes and ears' of security agencies.

India's Dominance in Indian Ocean Region

The Indian Ocean covers at least one fifth of the world's total ocean area. It is bounded by Africa and the Arabian Peninsula (known as the western Indian Ocean), India's coastal waters (the central Indian Ocean), and the Bay of Bengal near Myanmar and Indonesia (the eastern Indian Ocean). The Indian Ocean matters today, arguably more than ever. It is a major conduit for international trade, especially energy. Its littoral is vast, densely populated, and comprised of some of the world's fastest growing regions. The Ocean is also a valuable source of fishing and mineral resources. The Indian Ocean basin is of particular importance for India, as the region's most populous country and geopolitical keystone.

Importance of Indian Ocean Region (IOR)

- The region contains 1/3 of the world's population, 25% of its landmass, 40% of the world's oil and gas reserves.
- The most important trade routes of the world pass through this region. The Indian Ocean provides the predominant outlet for oil from the Persian Gulf to various destinations all over the world.
- The Malacca Strait is a critical choke point through which the oil bound for the West coast of USA, China, Japan, Australia and other countries of South-East Asia must pass. Oil being of vital interest to most nations, major powers, especially the USA, maintain a visible and credible presence in the region.
- The IOR is a critical waterway for global trade and commerce. This strategic expanse hosts heavy international maritime traffic that includes half of the world's containerized cargo, one third of its bulk cargo and two third of its oil shipment.
- Its waters carry heavy traffic of petroleum and petroleum products from the oilfields of the Persian Gulf and Indonesia, and contain an estimated 40% of the world's offshore oil production.
- Roughly 55 per cent of known oil reserves and 40 per cent of gas reserves are in the Indian Ocean region.
- Since dependence on oil will continue to increase in the future and exports from the Central Asian Republics by sea would also have to be routed through the ports of this region, the Indian Ocean is likely to witness clashes of economic interests and a turbulent security environment.
- India is one of very few (06) countries in the world to have developed the technology to extract minerals from the deep sea bed.
- India imports 70 % of its oil requirements, 4000 tankers come to Indian ports annually and almost 95 % of Indian trade moves by sea.
- Almost 5 million Indians work in Gulf countries and it is in India's interest to ensure that the environment in Gulf remains stable.
- In addition to providing precious minerals and energy source, the ocean's fish are of great importance to the bordering countries for domestic consumption and export.
- The region is home to continually evolving strategic developments including the competing rises of China and India, potential nuclear confrontation between India and Pakistan, the US interventions in Iraq and Afghanistan, Islamist terrorism, growing incidence of piracy in and around the Horn of Africa, and management of diminishing fishery resources.

Maritime Security; Indian Ocean and imperatives for India

- Location of Indian Ocean adjacency to Middle East, South Asia, Africa and South East Asia, make it important geographical space for major powers as a lot of oil and petroleum transport of world goes through the ocean.

- ❑ Major powers such as US, Britain, France, China always had their presence in the Indian Ocean, but due to increasing competitions between major powers, such as US-China and raising competition between regional and major powers, such as India-China, the region is becoming focus of regional and major powers maritime policies.
- ❑ India is a regional power adjacent to Indian Ocean, is a nuclear power and aspire to have dominance in Indian Ocean.
- ❑ India even considers Indian Ocean as its “backyard” and its policy makers considers that owing to its dominance in Indian Ocean, it would be able to exert power on not only regional countries but other countries adjacent to Indian Ocean.
- ❑ Therefore, in recent years India is procuring naval equipment such as UAVs, radars, helicopters missiles and building arms, vessels.
- ❑ It is also seeking refuge in pacts, arrangements and alliances, to facilitate the process further India recently decided to do a bureaucratic change as well by deciding to appoint a “National Maritime Security Coordinator”.

India's objectives in the Indian Ocean Region

- ❑ To spread its influence across the entire Indian Ocean Region, through trade and investment, diplomacy and strategic partnerships
- ❑ Upgrading relations with Africa, the Middle East and Southeast Asia; regions that hold mineral deposits and energy reserves critical to India's economic development and great power aspirations
- ❑ Positioning itself to emerge as the dominant Indian Ocean power in the decades ahead
- ❑ Ensuring that China does not gain a significant strategic foothold in the region
- ❑ Strengthening influence and control over Indian Ocean choke points through security relationships with key littoral states such as Singapore, Mauritius and Oman.
- ❑ 90% of India's international trade by volume is dependent on sea. India has been enhancing its strategic influence through the use of soft power, by becoming a major foreign investor in regional mining, oil, gas and infrastructure projects.

Need for a National Maritime Security Coordinator (NMSC)

- ❑ Indian maritime economic and security fragments are handled by different organizations, but it has been observed that due to their lack of coordination quicker decision making was not possible.
- ❑ Though India always wanted to have naval dominance and nuclear triad, it has not been aggressive in its commitments in the Indian Ocean.
- ❑ In recent deadly border conflict with China where Indian land forces are in very tight position and have no alternative to coerce PLA to withdraw from recently acquired positions along disputed LAC, development of strong naval force, building of naval alliances would help India in creating a pressure on China.
- ❑ As Chinese oil and petroleum and other exports go through the Indian Ocean, India with help of alliances wants to create a tougher situation for China to have some bargaining chip.
- ❑ India consider the IOR as its backyard hence, logically it is establishing a post dedicated solely for naval and maritime coordination and relations.

NMSC

- NMSC has been a long pending requirement since the Kargil GoM (Group of Ministers) recommended it and its need was most felt during the 2008 Mumbai massacre.
- In this unfortunate event, 10 Pakistani Lashkar-e-Taiba (LeT) gunmen directed by ISI handlers in Karachi intruded into Mumbai and created mayhem with the maritime security agencies like Navy, Coast Guard and Mumbai Port all at sea figuratively.
- The appointment of NMSC fills the need of the hour as the Navy, Coast Guard and state maritime boards all tend to work in silos with overlapping jurisdictions and are constantly at odds with each other.

NMSC responsibility:

- The task of coordinating between all the authorities concerned with maritime security and civil marine concerns will fall to NMSC. It will also be in charge of enhancing India's blue economy's necessities.
- It will examine every facet of maritime security and serve as the focal point for all problems associated with it. Additionally, it will be responsible for promoting greater communication between the many maritime authorities that operate separately.

Conclusion

The decision of the Union Government to create and appoint a National Maritime Security Coordinator (NMSC) to interface between the civilian and military maritime domain is a welcoming step. With the objective of enhancing security architecture and energy security of India, the NMSC will tie together hitherto fragmented nature of Civilian and military maritime architecture. The Maritime Security Coordinator will work under Indian National Security Advisor and be the principal advisor to the government on maritime security domain.

Border Area Issues of India with all the neighbours

The evolution of boundaries in the Indian subcontinent has a long historical legacy, which often has been a source of tension and conflict between neighbours. Before 1947, the Indian subcontinent was a single geographical unit comprising present day India, Pakistan, Nepal, Myanmar, Bangladesh and Sri Lanka, and marked by political, social and economic unity. People and goods were free to move anywhere in the subcontinent unhindered by barriers. However, political and administrative compulsions led to the division of the subcontinent and the eventual break-up of its social and economic unity as well. Boundaries hastily drawn to give shape to the new political entities did not follow any distinct physical feature. These superimposed lines cut across ethnic, social and economic communities, severing social and economic ties among the people straddling these new borders. Consequently, people of the same village often found themselves citizens of two different countries separated by a line. Their livelihoods were severely threatened by the disruption of trade as barriers were erected in the way of the smooth flow of cargo and passengers.

Some recent border dispute examples

- Face-off between Indian Army and China's People's Liberation Army (PLA) in the Doklam plateau, a disputed area of 89 sq km in western Bhutan, near East Sikkim. The crisis occurred on 8 June 2017,

when PLA troops crossed over to the Bhutanese territory with road construction machinery, with the aim of building a motorable road connecting Chumbi Valley and the Doklam Plateau.

- ❑ Border Area Development Programme (BADP) was initiated as early as 1987 along the India-Pakistan border to 'meet the special development needs of the people living in remote and inaccessible areas situated near the international border'.
- ❑ The construction of border fence by Myanmar has led to resentment among the people on both sides of the Indo-Myanmar border. The affected people mainly are Konyak, Khamti and Yimchunger Nagas who inhabit the areas of Eastern Nagaland in India and the Naga Self Administered Zone (NSAZ) in Myanmar.
- ❑ India and Bangladesh jointly inaugurated, Asia's largest Integrated Check-Post (ICP) at Petrapole, 95 km from Kolkata, in North 24-Parganas district of West Bengal. This is regarded as a landmark development towards strengthening bilateral trade as well as the border management process.
- ❑ At present, Bangladesh allows transit facilities to India's north-eastern states by waterways for cargoes and roadways for passengers. For transit through waterways, India and Bangladesh had signed the Protocol on Inland Water Transit and Trade (PIWTT).
- ❑ Actual Ground Position Line (AGPL), which divides the current position of Indian and Pakistani troops in the Siachen region. It is 110 km long and extends from NJ 9842 to Indira Col in the north.

Issues with neighbours

❑ Indian Bangladesh border

- Illegal Immigration – There were both push and pull factors working on this border. Under development, religious persecution, environmental concerns etc. pushed Bangladeshis into India, while India's huge economy and accommodative society pulled immigrants.
- Cattle and other Smuggling – It big unique problem with this border. It is said that if India restricts this supply then it can starve Bangladeshis of food. Cattle from as far as Haryana, UP, Bihar is taken to borders for grazing and then smuggled to Bangladesh. Bangladesh also imposes custom duty on these imports.
- Threat from Bangladesh assumes serious dimensions since it became a base for northeast insurgent groups like ULFA and Naga factions.

❑ India Pakistan Border

- This is spread across extreme climatic conditions given that the boundary runs from the hot Thar Desert in Rajasthan to the cold Himalayas in Jammu and Kashmir.
- Pakistan's policy of cross border terrorism, along with its intense hostile anti-India propaganda designed to mislead and sway the loyalties of border population.
- The intensification of cross border terrorism, targeted to destabilize India, has thrown up new challenges for our border management policy.
- The J&K cauldron is expected to continue.
- Vigorous efforts are on to revive militancy in Punjab.
- Illegal infiltration and smuggling of arms and explosives, narcotics and counterfeit currency are pressing problems.
- The guarding of the coastal and creek areas of Gujarat poses extreme challenges due to the hostile terrain, inhospitable climatic conditions, and hazardous nature of the sea and creek areas on this side of the border.

■ India China Border

- China appears to have become increasingly aggressive as it has steadily risen in power and as the influence of the West has progressively declined.
- China's defence cooperation and its support to Pakistan for missile technology are perceived in India to be threatening.
- The attempt by the People's Liberation Army (PLA) to escalate tension in the trijunction of the India-China Middle Sector of the boundary at Doklam is a new development.
- Bhutan's north-western region is close to Chumbi Valley and to the Tibetan region bordering the Indian state of Sikkim. A settlement between China and Bhutan in this area will have an obvious impact on Indian security.
- If Siliguri corridor is blocked, whole northeast will be cut off from India and that is a major concern and a security threat.

■ India Myanmar Boundary

- Free movement across the Indo-Myanmar border has been the practice from times immemorial due to the ethnic and cultural similarity in the areas adjoining the border.
- Illegal trade activities in a variety of contraband items flourish at Moreh on the Indo-Myanmar border.

■ India Nepal Border

- The dynamic nature of the problems concerning management of borders is brought out by the manner in which the sensitivity of India-Nepal border has changed over a period of time.
- This border, which has been an open one, was once peaceful and trouble-free.
- However, with the increasing activities of Pakistan's Inter-Services Intelligence (ISI) in Nepal, the nature of the border has changed completely.

■ India Bhutan Border

- The border areas on both sides of the Indo-Bhutan border do not have basic infrastructure such as communications, roads, health, education, drinking water facilities etc.
- These areas are often used as sanctuaries by the insurgent groups of the North East particularly the United Liberation Front of Assam (ULFA) and the National Democratic Front of Bodoland (NDFB).
- Settlements of Bangladeshis are coming up along either side of the Indo- Bhutan border.
- Many of them are reportedly seeking jobs and employment in the Bhutanese territory, in the garb of Indian citizens. This is another reason to closely monitor the Indo-Bhutan border.

Major Challenges

- Mass immigrations into India.
- Augmented cross-border terrorism.
- Penetration and ex-filtration of armed militants.
- Emergence of non-state actors.
- Link between narcotics and arms smugglers.
- Unlawful migrations.
- Left-wing radicalism.
- Separatist movements aided and abetted by external powers.
- Establishment of madrasas, which could result in security hazards.

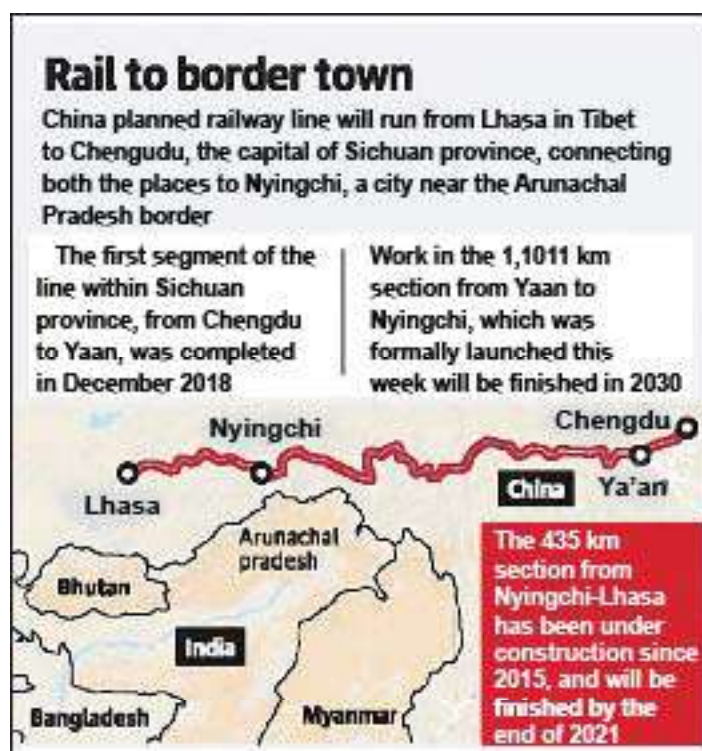
- Smugglers, drug-traffickers are often in association with local offenders, lower rung political leaders and police officials.

Suggestions

- Instead of high-cost and innovative technological solutions that require extensive technical expertise, a judicious mix of properly trained manpower and affordable and tested technology is likely to yield better results.
- Another method employed by the government to regulate the borders is the preparation of a national register and issuance of Multi-purpose National Identity Cards (MNICs). This would help to prevent illegal migration and facilitate the detection of those already staying in India.
- Fingerprints are the oldest and most widely adopted biometric technology used in smart identity management. As a result, this is the most mature of all biometric technologies.
- A smart inspection system uses a smart identity management system that ensures that only legitimate people are allowed to engage in cross-border management.
- To avert illegal immigration and other anti-national actions from across the border, Government of India has sanctioned erection of fencing/roads.
- The CIBMS is touted as a more robust and integrated system that is capable of addressing the gaps in the present system of border security by seamlessly integrating human resources, weapons, and high-tech surveillance equipment.
- Technical solutions are necessary to augment and complement the traditional methods of border guarding.
- They not only enhance the surveillance and detection capabilities of the border guarding forces but also improve the impact of the border guarding personnel against infiltration and trans-border crimes.

China's work on railway up to Arunachal border

- China has begun work on a strategically significant railway line - its second major rail link to Tibet - that will link Sichuan province with Nyingchi, which lies near the border with India's Arunachal Pradesh.
- The importance of the project, as per Chinese experts is two-fold. Like the Qinghai-Tibet railway line, which in 2006 connected Lhasa to the hinterland, this will be the second such route linking the Tibet Autonomous Region (TAR) to the hinterland.
- Secondly, it will run right up to Nyingchi near the border with India, which it will link to both Lhasa and Chengdu, the provincial capital of Sichuan. The entire line will run from Chengdu to Lhasa, connecting the two capitals of TAR and Sichuan and cutting the journey from 48 hours to 13 hours.



Concerns for India

- The India-China border dispute covers the 3,488-km-long Line of Actual Control, the de-facto border between the two countries. China claims Arunachal Pradesh as part of south Tibet which is firmly rejected by India.
- India is concerned about the strategic motivations that underlay China's construction and extension of railway lines along the border region, which is de facto marked by the Line of Actual Control (LAC). Chinese analysts have not been shy to point out that in the event of a war with India, the Chengdu-Lhasa railway line will help with the "delivery of strategic materials" right up to the disputed Sino-Indian border.

Government implements Shekatkar Committee recommendations related to creating border infrastructure

- Government has accepted and implemented three important recommendations of Committee of Experts (CoE) under the Chairmanship of Lt General D B Shekatkar (Retd) relating to border Infrastructure. These were related to speeding up road construction, leading to socio economic development in the border areas.
- On the matter related to creating border infrastructure, the Government has implemented recommendation of CoE to outsource road construction work beyond optimal capacity of Border Roads Organisation (BRO). It has been made mandatory to adopt Engineering Procurement Contract (EPC) mode for execution of all works costing more than Rs 100 crore.
- The other recommendation relating to introduction of modern construction plants, equipment and machinery has been implemented by delegating enhanced procurement powers from Rs 7.5 crore to Rs 100 crore to BRO, for domestic and foreign procurements. Border Roads has recently inducted Hot-Mix Plant 20/30 TPH for speedier laying of roads, remote operated hydraulic Rock Drills DC-400 R for hard rock cutting, a range of F-90 series of self-propelled snow-cutters/blowers for speedier snow clearance.
- New Technology like blasting technology for precision blasting, use of Geo-Textiles for soil stabilisation, cementitious base for pavements, plastic coated aggregates for surfacing, is also being used to enhance the pace of construction. With the empowerment of field officers through enhanced delegation of financial and administrative powers, there has been significant improvement in faster financial closure of works.
- The land acquisition and all statutory clearances like forest and environmental clearance are also made part of approval of Detailed Project Report (DPR).

Issues with Armed Forces

There is a widely sensed need for the rapid modernisation of the Indian armed forces, which is being reflected in some of the key initiatives that have been taken up by the Indian government so far (such as Make in India), so as to address to the complex security challenges that emanate from its hostile neighbourhood. However, the pace of modernisation of the Indian armed forces over the years has been rather slow, and technologically, they are not where they should have been. Indigenous development of modern defence hardware continues to remain a concern and Indian policy aspiration for defence self-sufficiency remains largely elusive.

- ❑ 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.
- ❑ Then there is inefficiency and apparent lack of accountability of various organs of the defence ministry responsible for indigenous design and manufacture of weapons.
- ❑ Lack of modernisation, capital outlay being the lowest in the last ten years.
- ❑ Pathetic understanding of matters military with political and bureaucratic decision makers, thus a general distrust on what they are asking Army to do.
- ❑ Lack of capital budget for new procurement schemes, especially 'big ticket' items, is another challenge.
- ❑ The politicisation of the Army is taking its toll on a soldier's psyche as he is forced to take sides, instead of remaining apolitical and secular in his thinking and action.
- ❑ Prolonged separation from the families, in an increasingly unsafe and polarised countryside.
- ❑ Lack of social and physical security of their kith and kins in home towns.
- ❑ 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.

Suggestions

- ❑ The Indian Army needs to undergo transformation and right-sizing towards becoming an optimised modern force, with a more efficient teeth-to-tail ratio.
- ❑ Enhanced jointness with the Air Force and the Navy, appointment of a Chief of Defence Staff (CDS) and formation of 'theatre commands' would definitely contribute to optimisation of resources.
- ❑ The Indian Army must fully operationalise the concept of the Reorganised Army's Multi-role Quick Reaction Force (RAMFOR) by creating a highly mobile assault division as a strategic reserve.
- ❑ The government must closely monitor capability building of the services, especially the Army, and vigorously support plans to address 'hollowness' of weapons, equipment and ammunition.
- ❑ The government must increase allocation for defence (excluding pensions) to 2.5 percent of GDP initially, and further raise it gradually to 3 percent until modernisation of the Armed Forces is complete.
- ❑ The government must stop protecting the defence public sector and create a genuine level playing field for entry of the private sector into indigenous defence manufacturing.
- ❑ India needs to progressively build capability of hard military power, soft power and demonstrated power in its quest to be recognised as a regional power with global influence.
- ❑ The Indian Army's deterrence posture must be based on flexible capability-based structures to deal with various forms and levels of conflict.

National Maritime Security Coordinator

- ❑ Vice Admiral G. Ashok Kumar (Retd.) has been chosen by the Indian government to serve as the nation's first National Maritime Security Coordinator (NMSC) in order to foster unity among many important stakeholders in the overall effort to defend the nation.
- ❑ **About NMSC:**
- ❑ Under the direction of National Security Advisor AjitDoval, NMSC has been appointed under the National Security Council Secretariat (NSCS). The NMSC position was developed as a follow-up to the Military Advisor position to get opinion on military-related issues. 2011 saw the creation of the position of military advisor.

- ❑ The NSA, who is also the secretary of the premier National Security Council presided over by the Prime Minister, is in charge of the NSCS.
- ❑ **NMSC responsibility:**
- ❑ The task of coordinating between all the authorities concerned with maritime security and civil marine concerns will fall to NMSC. It will also be in charge of enhancing India's blue economy's necessities.
- ❑ It will examine every facet of maritime security and serve as the focal point for all problems associated with it. Additionally, it will be responsible for promoting greater communication between the many maritime authorities that operate separately.
- ❑ **Need of NMSC:**
- ❑ More than twenty years ago, when the Group of Ministers (GoM) was established following the Kargil War, the need for NMSC was initially acknowledged.
- ❑ In its report, the Kargil Group of Ministers had advocated the creation of an apex body for the management of marine affairs in order to institutionalise connections between the Navy, Coast Guard, and the relevant Ministries of the Central and State Governments.
- ❑ Therefore, the GoM has requested that the Defence Ministry take the required steps to establish the top body. The Defense Ministry had suggested setting up a maritime security advisory board and appointing a maritime security advisor following the terrorist attacks on 26/11 in 2008. That, however, was postponed. The Cabinet Committee on Security finally approved the creation of the NMSC in November 2021.

Infrastructure Development in Border Areas

India is bordering 17 states having the international borders with Pakistan, China, Nepal, Bhutan, Myanmar and Bangladesh. This entire border comprised of unique topography, culture and varied socio-economic challenges. Considering unity of the nation and neighbourhood first policy of India, it is imperative to develop modern and competitive border road infrastructure.

Issues in Infrastructure Development in Border Areas

- ❑ Even after about 10 years of implementation of BADP, the border blocks are yet to be opened up and are in utter backwardness due to their isolation and inaccessibility.
- ❑ The State Government, though handicapped by its limited resources, is committed to accelerate the pace of development and is trying its best for development of the border areas.
- ❑ Presently, 10% of BADP fund allotted to the State Government is earmarked for security related schemes to be implemented by the state police and paramilitary forces and the balance 90% fund is equally distributed amongst the bordering blocks.
- ❑ National credit registry politics in Arunachal Pradesh, Sinhalese prosecution in Sri Lanka are some of the other domestic politics. Rough and difficult terrain, tough Weather and Climatic conditions, seismically active areas in most of the border, inadequate manpower, funds with Border Road organisation (BRO), Red-tapism and bureaucratic delays in projects also act as hindrance.

Suggestions for Infrastructure Development in Border Areas

- ❑ One of the most important advantages is development of legal and amicable trade relations with neighbouring countries. Examples of it are trade through Attari-Wagha border and Border Haats with Bangladesh and many more with Nepal, Bhutan, etc.

- ❑ Proper border road infra will reduce trafficking and smuggling, which is currently a big cause concern for India and neighbouring countries.
- ❑ Another major economic benefit is inclusive growth and development. Border road infrastructure, especially in harsh terrains such as northeast and Jammu & Kashmir provides avenue for self-employment and boost to traditional small scale Industries.
- ❑ Furthermore, tourism in Himalayas has not reached to its full potential due to improper road infrastructure. To tap full potential of natural tourism avenues we must further improve our border road infra.
- ❑ One of the major advantages is that through border road infra India will be successful in pushing for her ambitious neighbourhood first and act east policies. It will act as soft power in terms of creating people to people contacts. Best example of this is the most recent project of Kartarpur Corridor.
- ❑ Border road infra helps in maintaining peace and stability by controlling the security concerns related to inter-region and intra-region issues.
- ❑ The task of national integration which started with independence of India and still going on will be incomplete without border road infra. Connectivity and inclusivity are the important tools for national integration of far-flung areas such as Northeastern states and Ladakh, etc.
- ❑ Another important advantage of border roads is in proper and swift disaster management. Difficult and harsh terrains of Indian borders and relatively low development of bordering countries make it inevitable for India to prepared and self-sufficient to handle any kind of disasters.

High altitude pseudo-satellites (HAPS)

- ❑ High altitude pseudo-satellites (HAPS) are systems or platforms that usually float or operate for long periods, sometimes for months, at about 20 km above the Earth's surface. This puts them in the range of the stratosphere, where these heights can put them above commercial aircraft and at heights that avoid turbulence and moisture.
- ❑ The growth of unmanned aerial vehicles (UAVs) and cheap satellites in recent years has prompted scientists, researchers, military and business interests to look at systems that operate in between or are a hybrid of UAVs and satellites.

How are they Beneficial for the Military?

- ❑ India has been working towards uplifting its space capabilities and focusing on the small satellite (SmSats) segment to fill the capability and performance limitations in meeting the C4ISR (Command, Control, Computers, Communications, and Intelligence, Surveillance and Reconnaissance) needs vital for military operations. HAPS, due to their affordability, versatility and ability to provide prolonged high-resolution coverage of specific areas can play a vital role in supplementing defence communication infrastructure both territorial and space based to render robust round-the-clock surveillance on the borders and in the Indian Ocean region.

Benefits of Pseudo-Satellites

- ❑ **Flexibility:** Pseudo-satellites are far easier to launch than traditional aircraft. Requiring no runway or airport, they can be launched and piloted to wherever they're needed.
- ❑ **Durability:** This type of satellite is entirely solar powered, meaning it can operate independently for up to 25 days. Made of carbon fibre, the model is strong while remaining light enough to fly, powered by a lithium-sulphur battery.

- ❑ Connectivity: The satellites can stay focused on a specific area of interest which can be hundreds of miles wide.

Security threats posed by drones

- ❑ Law enforcement organisations throughout the world are increasingly more concerned about the possible use of drones in a terrorist event or assault against critical infrastructure and soft targets as drone technology becomes more widely available globally.
- ❑ For instance, the Houthi rebels in Yemen recently claimed responsibility for a drone attack in Abu Dhabi that claimed the lives of three people, including two Indian citizens. In response, the UAE government has ordered a month-long ban on all private drone and light sport aircraft operations in the Gulf nation.

About Drones:

- ❑ Unmanned aircraft is known as a drone in common parlance (UA). Drones, which were first created for the aerospace and military sectors, have become widely used because to the increased levels of efficiency and safety they bring.
- ❑ The level of autonomy of a drone can range from remotely piloted, in which case a person controls its movements, to advanced autonomy, in which case it relies on a network of sensors and LiDAR detectors to determine its movement.

Significant is Drone Technology in India

- ❑ Drones are currently giving countries considerably more economic and commercial viability, and the industry is benefiting greatly from the easy availability of these drones at affordable prices. The following industries make use of drone technology:
- ❑ Defense: The deployment of drone systems as a symmetrical weapon against terrorist assaults is possible. The national airspace system can incorporate drones.
- ❑ Goals of Healthcare Delivery: The Telangana government and the Ministry of Civil Aviation have approved a scheme to use drone technology to deliver immunizations in outlying districts.
- ❑ Drones can be used to spread pesticides and micronutrients in the agricultural industry. Recently, Standard Operating Procedures (SOPs) for drone application in agriculture were published by the Ministry of Agriculture & Farmers Welfare.
- ❑ Drone technology was employed for real-time asset and transmission line surveillance, theft prevention, visual inspection and maintenance, construction planning and management, and other purposes in the SVAMITVA program that the Indian government introduced.
- ❑ Drones for mining are employed in challenging monitoring situations at industrial facilities that may include toxic gases, high temperatures, or high pressure and are impossible for humans to access.

What exactly is anti-drone technology?

- ❑ The term “counter drone technology” describes devices that are used to track and/or thwart unmanned aircraft systems while they are in the air. As drones become more widely used, technology is quickly developing and changing. The growing worry over the threat that drones pose in both military and civilian settings can be attributed to its expansion.

- Many nations are investing money to create these technologies, such as the US DOD (United States Department of Defense), which has set aside only 83 million dollars for the purchase of ground-based drones, and anti-drone systems and roughly 404 million dollars for research and development.
- A counter drone system is also being developed for the airborne system, at a cost of roughly 85 million dollars. India has created a soft kill counter-drone system through industry, and a hard and soft kill system through the DRDO.
- The use of jammers to stop the drones' communication, interference with GPS signals, or spoofing of such signals are examples of soft kill or non-kinetic defenses against drone strikes. Bullets or firearms are used as kinetic or "hard-kill" tactics to interfere with drones' workings.

What is the Security Risks Associated with Drone Technology?

- Terrorists have employed drones in a number of occasions over the past few years to plot and carry out planned and attempted strikes across the globe.
- Along its western border with Pakistan, India has seen a rise in rogue drone activity in recent years, with drones dumping weapons, ammunition, and drugs as well.
- In June 2021, drones were employed for the first time to drop explosives, setting off explosions inside the technical sector of the Air Force Station in Jammu.
- A bigger populace can buy drones thanks to lower prices. The main factor driving the rise of drone assaults is that they are significantly less expensive than conventional weapons while producing far more destructive effects.
- The potential for combat drones to be used to carry WMD makes them particularly dangerous. There are significant risks when non-state parties buy combat drones.

Way Ahead:

- Countering Cross-Border Strikes: India would continue to place more emphasis on preventing drone cross-border attacks. Only with the aid of technology will such drone attacks be able to be defended against. Drone and anti-drone technologies are both in development, and India must stay up. The government will need to step in at this point with a budget to force the stakeholders to concentrate on anti-drone technology.
- Israel and the United States are also two of the world's top manufacturers of military drones. It is possible to take advantage of the bilateral relationships to persuade them to help with the purchase and continued production of military drones. The government's encouragement will hasten the advancement of drone technology.
- Immediate Areas of Focus: India needs but is now unable to provide defense against drone attack drones. It is a newly developed aspect that will take time to counter; therefore the government can act right now by identifying some key areas of importance and concentrating all drone defense synergies in those regions. These locations may include airports, VIP zones in cities, etc.
- Technology to combat drones the threat comes from renegade elements rather than drones. Drone strikes are undoubtedly a possibility while they are in use, but ceasing their use altogether is not the answer. The creation of counter drones is the key to solving this issue.
- To watch threats, particularly those near vital assets, India must invest in its own Unmanned Aerial Vehicle (UAV) systems and counter-drone technologies. One anti-drone system, being developed by the DRDO, is already operational.

DEFENCE PROCUREMENT

Working Analysis of Defence PSU

- India has eight Defence Public Sector Undertakings (DPSUs) under the control of Department of Defence Production, Ministry of Defence (MoD). These Undertakings together with 39 Defence Ordnance Factories (OFs) form the backbone of India's defence production, and are responsible for making India self-sufficient in defence production.
- The necessity of establishing DPSUs was to meet advanced weapons and equipments required by the armed forces, and work towards the goal of self-reliance in defence production.

Important achievements of Indian DPSUs

- Hindustan Aeronautics Ltd (HAL), India's premier defence aerospace manufacture is developing systems like Tejas, Dhruv ALH, Light Combat Helicopter, and the Light Utility Helicopter and licensed production of Su-30Mki.
- The Defence Research & Development Organisation (DRDO), set up to "develop cutting-edge technologies for the armed forces", has a mind-boggling total production value of Rs 2, 60,000 crore. It along with ADA (Aeronautical Development Agency) is developing and has designed the Tejas, and is to start design work on the Advanced Medium Combat Aircraft (AMCA). The AMCA is to incorporate fifth-generation technology, including stealth – not excluding radar-absorbent paint. DRDO has also developed Airborne Early Warning and Control (AEW&C) system, missile systems for defense forces.
- Bharat Electronics Limited (BEL) makes defence electronics for every Indian aircraft, naval ship, and missile and land vehicles. Its much diversified product range includes radars, electronic warfare equipment, Identification Friend or Foe, Head-up Displays, and electro-optical devices. Such products have also been used to upgrade older aircraft like the Jaguar and Mirage 2000. It has developed Digital Flight Control Computer and the Radar Warning Receiver for Tejas.
- The Council for Scientific and Industrial Research had set up the National Aerospace Laboratories (NAL) for research and development as well as design work.

Issues in their performance

- India is the largest importer of arms and account for 15% of total arms imports. This shows the gap between the requirement of defense modernization and indigenous capabilities, which has to be filled by DPSUs.

- HAL still needs to enhance quality control as well as maintainability and reliability of its products, some of which, like the Intermediate Jet Trainer, have fallen by the wayside.
- Navy has declined LCA-Tejas Naval version on grounds of its weight. Also Tejas is more suitable for air-defense but performance lacks in areas of payload capacity and range.
- HAL still does not have an in-house design capability for engines. That is to be rectified with the design of two technology demonstrators, the HTFE-25 turbofan and the HTSE-1200 turboshaft helicopter engine. HAL could, some day, develop large engines for fighters and helicopters of its own design. Attempts to develop Nirbhay, subsonic missile have also not been fruitful.
- Indian exports in the defence sector are meager, which also indicates the poor capabilities of Indian DPSUs. Though Indian exports in Missile were restricted because of Missile Technology Control Regime, but still they were far below.
- DPSUs in general suffer from low productivity compared to their counterparts in the global defence industry.

Major suggestions and steps taken

- Make in India and Defence Procurement Policy initiatives of GoI are aimed at improving the manufacturing ecosystem in India. Focus on IDDM (Indigenously Designed, Developed and Manufactured) as the most favored route of procurement in defence acquisitions will benefit DPSUs.
- Focus on co-production and transfer of technology from foreign producers for example in Brahmos, Barak missile, Rafale fighter is going to improve the technological know-how of the Indian DPSUs, which will improve their capacities in the long run.
- There are accusations of too much interference in the functioning of DPSUs, which affect their human resource planning, project planning and results into failures and cost escalations of projects. Therefore these must be provided with operational autonomy with consequent accountability mechanisms. The example of ISRO must be taken to turn around the DPSUs.
- Shekatkar Committee has recommended the performance audit of non-combat units of Ministry of Defence and this should be done quickly to analyze the shortcomings in DPSUs.
- Collaborations with industries, international organizations must be focused to provide synergies in defense production.

Defence Research and Development Organisation (DRDO)

- Defence Research and Development Organisation (DRDO) is charged with military's research and development. It covers various fields like aeronautics, armaments, electronics, land combat engineering, life sciences, materials, missiles, and naval systems etc. With 52 laboratories engaged in developing cutting edge technologies, DRDO has achieved significant work in the past. The recent launch of Intercontinental ballistic missile Agni 5, DRDO put India in the coveted group of countries achieving intercontinental missile range.

Highlights and Achievements

- DRDO's most notable achievement has been the completion of the Integrated Guided Missile Development programme in 2008. It was mainly led by Dr. APJ Abdul Kalam and included missiles such as – Agni, Nag, Trishul etc.

- ❑ DRDO besides developing military related technologies, has developed technology to aid everyday civil life. For example –chikungunya Elisa detection kit, bio-emulsifier for bioremediation etc.
- ❑ DRDO often engages with India's defence partners to develop cutting edge technology or to conduct joint research. Example – Russia.
- ❑ DRDO often develops technologies that aid Government of India's schemes or programmes. Example – DRDO developed a bio digester to solve the problem of untreated human waste.

Shortcomings and Challenges

- ❑ Ministry of Defence has been slow in making appointments to the top positions in DRDO. In the recent past the organisation remained headless for few months.
- ❑ DRDO's annual budget is very low and very less when compared to budgetary allocation made to military research by other countries, especially China.
- ❑ India recently called off a defence partnership with Russia to develop 5th generation fighter aircraft.
- ❑ Slow indigenous development when compared to other countries.

Way forward

- ❑ Defence analysts sometimes highlight the possibility of two front wars. With China's rapid stride in defence capabilities, India should pay close attention to defence research and indigenous developments.
- ❑ Budgetary allocation to DRDO and timely appointments of its head will ensure both requisite resources and leadership.
- ❑ DRDO has proved to be an exemplary establishment capable of delivering quality indigenous technologies. It has proved to be a premier institution devoted in both military and civil related research and development.

Hindustan Aeronautics Limited

Hindustan Aeronautics Limited is a government owned establishment involved in aerospace and in design, fabrication and assembly of helicopters, aircrafts, jet engines etc. HAL has been in news mainly related to defence and Aerospace related developments. Hindustan Aeronautics Limited (HAL) has recently built an indigenous supersonic aircraft Tejas which has been inducted into the Indian Airforce. In the recent past HAL has developed many indigenous technologies and aided in India's defence capabilities.

Achievements

- ❑ International partnerships – more than 40% of HAL's revenues comes from international deals in manufacture aircraft. Example – kamakov attack helicopter in partnerships with Russia.
- ❑ Fifth generation aircraft – it has a deal with Sukhoi Corporation of Russia to develop a fifth-generation fighter aircraft.
- ❑ Dhruv helicopter – it is a utility vehicle developed by HAL. It has transport, utility, reconnaissance and medical evacuation variants.
- ❑ Tejas aircraft – HAL developed the Tejas under the Light Combat Aircraft programme to replace the agent fleet of Mig-21.
- ❑ Unmanned Aerial Vehicles (UAV)- Nishant UAV, Rustom UAV etc. are also manufactured under the guidance of HAL.
- ❑ Apart from it reconnaissance aircrafts, transport and passenger aircrafts etc. are also manufactured.

Challenges

- Delay in payment of wages-HAL made news recently related with delay in payment of mechanics.
- Slow indigenous development –according to defence experts deliveries are too slow and indigenous development has been less than satisfactory.
- Poor Competition- HAL has near monopoly in the field of aerospace and related manufacturing. This leads to poor competition and lack options for procurement for government
- Private lobbies are trying to stop indigenous defence manufacturing and facilitate privatisation according to some experts.

Way Forward

- MSMEs to be promoted - Medium small and Micro Enterprises should be promoted in few areas in order to promote MAKE IN INDIA. This will also help to provide say spare parts and services quickly and hence speed up production.
- Open to private players– other private players should be allowed to enter aerospace industry (with adequate safeguards). This will promote competence and boost efficiency of HAL.
- Hindustan Aeronautics Limited is one of the largest aerospace companies in Asia. As the only big name in aerospace industry, it has delivered quite well but sometimes suffered roadblocks.
- All the stakeholders – defence ministry, scientists and bureaucrats- should come together to iron out challenges and promote indigenous development of aerospace defence industry.

Atmanirbhar Bharat

Recently, the Prime Minister outlined Rs.20 lakh crore stimulus package which was accompanied with large scale structural reforms. Prime Minister in his address stated that India's self-reliance does not advocate self-centric arrangements. It is ingrained in the happiness, cooperation and peace of the world. It has been clearly specified that this idea of self-reliance is not about a return to the era of import substitution or isolationism. The Ministry of Defence will introduce import embargo on 101 items beyond given timeline to boost indigenisation of defence production, Defence Minister announced recently, while stating it as a big step towards 'Atmanirbhar Bharat' (self-reliance) in defence

Issues

- The package of Rs 20 lakh crore comprises both fiscal and monetary measures, the latter being in the nature of credit guarantees and liquidity infusions into banks and other financial sector institutions rather than the economy per se.
- Majority of the package is liquidity measures that are supposed to be transmitted by RBI to Banks and Banks to Citizens. This transmission wouldn't be as smooth owing to inefficient transmission of monetary policy.
- The lockdown has lowered aggregate demand, and a fiscal stimulus is needed. However, the package, by relying overwhelmingly on credit infusion to boost the economy, has failed to recognise that investment will pick up only when people across income segments have money to spend.
- Unless the rest of the domestic economy is revived, the MSME sector may face a shortage of demand, and its production may soon sputter to a close.
- Government claims that the stimulus package is around 10% of India's GDP. However, financing it would be difficult as the government is worried about containing the fiscal deficit.

- ❑ The government seeks a disinvestment to mobilise the finances for the plan. However, the majority of Indian industries are already a bit debt-laden to take up the stake in PSUs. Further, it is difficult to borrow the foreign markets, as rupee with respect to dollar is all time low.

Suggestions

- ❑ The economic package for the country emerging out of the lockdown requires a stimulus enhancing demand across the economy.
- ❑ The best way for this is to spend on green field infrastructure.
- ❑ Infrastructure spending uniquely creates structures that raise productivity and extends spending power to the section of the population most affected by the lockdown, namely daily wage labourers.
- ❑ For financing of the stimulus package, India's foreign reserves stand at an all-time high which could be strategically used to finance its needs. The rest may have to come from privatisation, taxation, loans and more international aid.
- ❑ Any stimulus package will fail to reflect the trickle-down effect, until and unless it is backed by reforms in various sectors.
- ❑ Thus, Atma nirbhar plan also encompasses the unfinished agenda of holistic reforms which may include reforms in Civil services, Education, Skill and Labour, etc.

Technological Dependence on Other Nations

- ❑ The phenomenon of technology transfer has existed ever since the beginning of technological progress. Having significantly increased in recent years, it will probably attract the world's attention for many years to come. Many developing countries now appear to be seeking technological progress through technology transfer to realize development in a much shorter time than that required originally by developed countries. Technological dependence could be considered the opposite of self-reliance. One transparent indicator of its existence is a situation in which the major source of a country's technology is abroad. When a country imports from a single country, it has a very high degree of technological dependence.

Issues with Technological dependence on other nations

- ❑ As Information and Communication Technology infrastructure is the backbone of many frontier technologies, there is a risk of its triggering a new frontier technology divide, compounding an already existing digital divide.
- ❑ An estimated three billion people could still lack internet access by 2023, and many more will have little or no opportunity to reap the benefits of digital technologies.
- ❑ Frontier Technology per se is not the problem, but there are ethical issues surrounding privacy, ownership and transparency.
- ❑ Developing countries, in particular, are starting from a difficult position, because they are already grappling with the challenges of low human capital, ineffective institutions, and a difficult business environment.
- ❑ The system is also largely run by scientists-turned-bureaucrats and "nepotism, patronage culture" are prevalent.
- ❑ Also, the prevalent incompetence across the spectrum has taken a toll on 'peer reviewing' where incompetent scientists get to reinforce their mediocrity.

- ❑ There is a culture of elitism in our labs, where the manual work is done by lab assistants and scientists mostly just command orders.
- ❑ Also, rather than contributing to social debates, Indian scientists shun public commentary, unless it is to serve as government spokespersons.
- ❑ Currently, it has been observed that, small elite research institutions get most of the grants, while universities get very less research funds.
- ❑ Due to funding constraints, almost all the significant work from India is in the theoretical domain, as these are less burdened by money requirements.

Suggestions for Technological dependence on other nations

- ❑ With globalisation, it is easier to notice the growing contrast between the designs for promoting innovation in the western world and in India.
- ❑ Having a young population and a strong Diaspora that is more affluent than any other country, India has the potential pioneering high-tech innovation.
- ❑ As a first step, it is important to acknowledge the significant contributions of Indian scientists abroad and capitalise on their learning through collaboration.
- ❑ The technology policy recognised the importance of perspective planning in advance for the development of relevant technologies in all areas of priority.
- ❑ It called for the use of science and technology for employment generation, fulfilling energy requirements, improving the efficiency and productivity of public sector enterprises, development of improved technologies for food, housing and industry, and for the development of environment friendly technologies etc.
- ❑ Importance to the up gradation of indigenous technologies to prevent their obsolescence.
- ❑ To ensure that the message of Science and technology reaches every Indian including women and children, and to promote scientific temper among them.
- ❑ To utilize Science and technology for food, agriculture, environment, energy security, and poverty alleviation programmes.
- ❑ To promote scientific research in academic Institutions and Universities, and provide them necessary autonomy for research and development.
- ❑ To promote the empowerment of women in science and technology activities.
- ❑ To encourage innovation for economic development and strengthen the enabling mechanism related to technological development. To establish an Intellectual Property Rights (IPR) regime for the protection of intellectual property and its commercialization.
- ❑ To ensure the availability of high-speed access to information through scientific development in digital technologies.
- ❑ To utilise the new technologies for the purpose of disaster management and for the prevention of natural hazards such as cyclones, floods, drought, landslides, and earthquakes etc.
- ❑ Promotion of scientific temper and its spread among all the sections of society.

Decoupling India's Manufacturing with China

The border clashes with China and the COVID-19 pandemic has given way to concerns on India's dependence on Chinese manufacturing. In this context, here is an assessment if India could really decouple itself from Chinese manufacturing and the options before it.

Issues

- ❑ India is dependent on China regarding capital goods. This includes a wide variety of machinery, including electrical machinery, semiconductor driven machinery sector, etc.
- ❑ Thus, the ban on Chinese imports will affect the competitiveness of domestic manufacturing, and thus further erode the country's export competitiveness.
- ❑ India accounts for a minuscule share of China's export market; it will have a limited impact on China.
- ❑ Any attempt to reduce imports from China, operationalised through tariffs or other non-tariff barriers, will raise prices for Indian consumers.
- ❑ The poorest consumers will be the worst-hit in a trade ban of this kind because they are the most price-sensitive.
- ❑ There is also the issue of Chinese investment in the Indian start-up space to contend with. Companies like Alibaba and Tencent have invested in Indian unicorns such as Zomato, Paytm, Byju's, Ola cabs and others.
- ❑ It's important to note along with being an exporter of assembled final products, China has also over the years become a major consumer for final products.

Suggestions

- ❑ India's strategy should be to boost manufacturing competitiveness and increase its share in world trade.
- ❑ In this pursuit, there is a need to create an infrastructure that raises the competitiveness of India's exports.
- ❑ There is a need to push through long-pending legislation that aims to address the structural bottlenecks (in 4Ls: Land, Labour, Law, Liquidity) that continue to plague and hinder domestic competitiveness.
- ❑ In spite of banning Chinese imports, India should tackle trade by trade. India can lobby for a more liberalised service sector in China.
- ❑ In spite of drawing border disputes into a trade dispute, India should reply to China strategically in such matters of strategic importance.

Modernisation Fund for Defence and Internal Security (MFDIS)

- ❑ The 15th Finance Commission has recommended constitution of a dedicated non-lapsable Modernisation Fund for Defence and Internal Security (MFDIS) to bridge the gap between projected budgetary requirements and allocation for defence and internal security.
- ❑ The indicative size of the MFDIS for 2021-26 is ₹2,38,354 crore and the maximum recommended.
- ❑ However, the unutilised amount from the normal budgetary allocations to the Ministry of Defence (MoD) and the Ministry of Home Affairs (MHA) for capital expenditure shall not be part of the Fund. The Defence Ministry has for long been demanding a non-lapsable fund keeping in view the long trajectory of military modernisation.
- ❑ The Finance Commission said the fund will have four specific sources of incremental funding which include transfers from the Consolidated Fund of India, disinvestment proceeds of defence public sector undertakings (DPSUs), proceeds from the monetisation of surplus defence land, including realisation of arrears of payment for defence land used by State governments and for public projects and cost

recovered of encroached land and proceeds of receipts from defence land likely to be transferred to them and for public projects in future.

- As per the Commission, the proceeds will be utilised for capital investment for modernisation of defence services, capital investment for the Central Armed Police Forces (CAPF) and modernisation of State police forces as projected by the MHA and a small component as welfare fund for soldiers and para-military personnel.

Defence Production and Export Promotion Policy 2020

- In order to provide impetus to self-reliance in defence manufacturing, multiple announcements were made under 'Atmanirbhar Bharat Package'. In implementing such framework and to position India amongst the leading countries of the world in defence and aerospace sectors, Ministry of Defence (MoD) has formulated a draft Defence Production and Export Promotion Policy 2020 (DPEPP 2020). The DPEPP 2020 is envisaged as overarching guiding document of MoD to provide a focused, structured and significant thrust to defence production capabilities of the country for self-reliance and exports.
- **The policy has laid out following goals and objectives:**
 - To develop a dynamic, robust and competitive Defence industry, including Aerospace and Naval Shipbuilding industry to cater to the needs of Armed forces with quality products.
 - To reduce dependence on imports and take forward "Make in India" initiatives through domestic design and development.
 - To promote export of defence products and become part of the global defence value chains.
 - To create an environment that encourages R&D, rewards innovation, creates Indian IP ownership and promotes a robust and self-reliant defence industry.
- **The Policy brings out multiple strategies under the following focus areas:**
 - Procurement Reforms
 - Indigenization & Support to MSMEs/Startups
 - Optimize Resource Allocation
 - Investment Promotion, FDI & Ease of Doing Business
 - Innovation and R&D
 - DPSUs and OFB
 - Quality Assurance & Testing Infrastructure
 - Export Promotion

MILITARY POLICIES ACROSS THE GLOBE

Nuclear Arms race Issues

Arms race is a pattern of competitive acquisition of military capability between two or more countries. The term is often used quite loosely to refer to any military buildup or spending increases by a group of countries. The competitive nature of this buildup often reflects an adversarial relationship. The arms race concept is also used in other fields.

Issues

- ❑ Arms races are frequently regarded as negative occurrences in both economic and security terms.
- ❑ Even for arms-producing countries, excessive military expenditure is likely eventually to have negative economic consequences.
- ❑ An arms race may heighten fear and hostility on the part of the countries involved.
- ❑ States can defy in numerous ways with very low risk of detection.
- ❑ Strategic competition among major powers is today's norm.
- ❑ While the risk of large-scale, world-ending nuclear war has declined, regional instability, the proliferation of weapons and the materials to make them along with emerging threats like cyber and terrorism mean the risk of a single nuclear weapon or device being detonated - by accident, by miscalculation or on purpose - is on the rise.

The revival of the nuclear arms race

- ❑ End of the unipolar world for the US: The key change from the 1990s is that the U.S.'s unipolar moment is over and strategic competition among major powers is back.
- ❑ The U.S. now identifies Russia and China as 'rivals'.
- ❑ Its Nuclear Posture Review asserts that the U.S. faces new nuclear threats because both Russia and China are increasing their reliance on nuclear weapons.
- ❑ The U.S., therefore, has to expand the role of its nuclear weapons and have a more usable and diversified nuclear arsenal.

- ❑ The Trump administration has embarked on a 30-year modernisation plan with a price tag of \$1.2 trillion, which could go up over the years.
- ❑ Concerns of Russia and China: Russia and China have been concerned about the U.S.'s growing technological lead particularly in missile defence and conventional global precision-strike capabilities.
- ❑ Russia has responded by exploring hypersonic delivery systems and theatre systems while China has embarked on a modernisation programme to enhance the survivability of its arsenal which is considerably smaller.
- ❑ Cyber capabilities being increased: In addition, both countries are also investing heavily in offensive cyber capabilities.
- ❑ The New Strategic Arms Reduction Treaty (New START) limits U.S. and Russian arsenals but will expire in 2021
- ❑ And U.S. President Donald Trump has already indicated that he does not plan to extend New START.
- ❑ Instead, the Trump administration would like to bring China into some kind of nuclear arms control talks.
- ❑ But China has avoided such talks by pointing to the fact that Russia still account for over 90% of global nuclear arsenals.

Some of the Nuclear Treaties

- ❑ Convention on Nuclear Safety
- ❑ Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste management
- ❑ Treaty on the Non-Proliferation of Nuclear Weapons (NPT)
- ❑ South Pacific Nuclear Free Zone Treaty (Rarotonga Treaty)
- ❑ Treaty on the Southeast Asia Nuclear Weapon-Free Zone (Treaty of Bangkok)
- ❑ Partial Nuclear Test Ban Treaty (PTBT)
- ❑ Conference on Disarmament (CD)
- ❑ Comprehensive Nuclear-Test Ban Treaty
- ❑ Fissile Material Cut-off Treaty (FMCT)

India's Soft Power

Power in International Relations (IR) is defined in relational terms, as the ability of actor A to influence the behaviour of actor B to get the outcome he wants. That is to say, there is no absolute power. Traditionally, military and economic powers were considered the major factors. However, some other intangible aspects have also been given importance by many strategic thinkers even in the past. The term Soft Power was first used by the eminent IR scholar Joseph Nye in his book "Bound to Lead: The Changing Nature of American Power." In the book, he identified three dimensions of power; coercion by military force, influence by offering economic incentives and finally the ability to co-opt other states by the nation's appeal based on its culture and values. The argument is that other states modify their preferences because of their favourable perception of you.

Issues

- ❑ India has a high number of UNESCO World Heritage sites, but still fares poorly on tourism and education on a per capita basis.

- ❑ Buddhism has hundreds of millions of adherents around the world but very few in its birthplace in India. While Buddhism has become indigenized in such places as Japan, Thailand, Sri Lanka and Mongolia, India has only recently made efforts at appealing to these countries as the fount of Buddhism, by facilitating pilgrimages and sponsoring religious renovations, in China and Myanmar.
- ❑ Most Indian cultural diffusion to overseas audiences has occurred without the involvement of the Indian government.
- ❑ Though India may be home to more top 30 unicorns (billion-dollar start-ups) than any country (other than the United States and China), its digital penetration remains low, with millions of its population still without access to electricity, and basic digital technologies.
- ❑ India rates badly on any measure of state-driven cultural diffusion rather than the more organic and natural private sector and citizen-led efforts.
- ❑ India was plagued by impoverishment, missing out on positive associations, coupled with lack of investment in cultural diplomacy, a reputation of deep-rooted corruption, hostile business environment, red-tapism, lack of infrastructure and severe pollution in urban areas.

Suggestions

- ❑ Soft power enables a change of behaviour in others, without competition or conflict, by using persuasion and attraction. Soft power can, no doubt, play a vital role in producing benevolence.
- ❑ It has the capacity to influence broader international audiences at large, in shaping the perceptions about the legitimacy and influencing environment of the permissive boundaries in which economic and military power is used.
- ❑ Even in the ancient time's scholars like Kautilya and Kamandak had advocated the use of soft power for achieving progress in state affairs.
- ❑ A country's soft power influence rests on how effectively it uses resources of culture, values, and economic policies.
- ❑ Soft power is power and at times, it is more powerful than hard power.
- ❑ A separate revitalized ministry was established to address the concerns of the outside Diaspora and re-establish their Indian connect so as to make them active participants in the extension of the country's goodwill and influence.
- ❑ The government was also successful in projecting yoga and Ayurveda as quintessentially Indian legacy. Recognition by UN of June 21, as International Yoga Day on the insistence of Indian government has been a step in the right direction.
- ❑ India has also projected itself as a crusader of environment protection and taken a strong stance against climate change.

Open Skies Treaty

Recently, the United States of America (USA) has announced that it will exit the Open Skies Treaty (OST) due to continuous violation of the treaty by Russia and changes in the security environment. It was signed in 1992 and came into effect in 2002. It is an agreement that allows its 34 signatory countries to monitor arm development by conducting surveillance flights (unarmed) over each other's territories. Therefore, the treaty established an aerial surveillance system for its participants. Both USA and Russia are signatories of the treaty. India is not a member of this treaty.

Issues

- ❑ The OST exit is only the recent example in the list of important pacts that US has stepped away from during the Trump presidency.
- ❑ The US has already stepped away from pacts such as the Paris Agreement and the Iran nuclear deal.
- ❑ Experts are now contemplating the fate of the US-Russia 'New START' nuclear arms control agreement, which will expire in February 2021.
- ❑ Trump has already said that his administration would not renew the treaty unless China joins.
- ❑ Many see this as improbable, given the already heightened tensions between USA and China over the pandemic.

Suggestions

- ❑ The OST was signed in 1992, much before the advent of advanced satellite imaging technology, which is currently the preferred mode for intelligence gathering.
- ❑ Yet, surveillance aircraft provide key information that still cannot be gathered by satellite sensors, such as thermal imaging data.
- ❑ Also, since only the US has an extensive military satellite infrastructure, other NATO members would have to rely on US to obtain classified satellite data.
- ❑ This satellite data would be more difficult to obtain compared to OST surveillance records that have to be shared with all members as a treaty obligation.
- ❑ Notably, the OST's utility for U.S. is that since 2002, it has flown 201 surveillance missions over Russia and its ally Belarus.
- ❑ A former Trump official had also hailed OST data gathered during the 2014 Russia-Ukraine conflict.

Women into Military Police

The decision could be the first step before including women for combat duties. It will help in analyzing the implications of their induction on bigger frame. There are allegations of gender specific crimes against army; this prompted the need for induction of women in the military police. During operations in Kashmir, the Army has often confronted women protesters and women soldiers can handle such situation effectively.

What are some of the arguments cited against offering women officers' combat roles?

- ❑ First, it is said that because of physical or biological reasons, women officers cannot sustain the rigour or enduring powers required in the rough terrains of the battlefields. Being smaller and lighter than their male counterparts, these women officers have almost half the latter's upper body strength and 25-30 percent less aerobic capacity. Besides, the female skeletal system is more prone to fractures.
- ❑ Psychologically more kind-hearted and compromising, the women fighters cannot take tough decisions easily, particularly while dealing with ground forces as fighter pilots (bombing them for instance). They also need more space and privacy (separate toilets and sleeping arrangements) which can be premium, particularly in platforms like submarines.
- ❑ It has been seen that most women officers like peace-time postings with their families. They need more leaves from duty to attend to the ailing family elders and children's education, let alone the normal maternity leaves from time to time.

- ❑ That is why, so this line of argument is, women officers in our armed services should be in roles that do not require physical hardships such as commanding troops, flying fighter jets and manning battle ships and submarines. Instead, they can do more meaningful roles as nurses, doctors, engineers, architects, intelligence officers, cyber experts and legal officers, roles that are as important as the combat ones for the armed forces.
- ❑ There is possibility of their physical abuse or molestation by the enemy in case they are wounded or taken as prisoners.

What are some of the arguments cited in favour of offering women officers' combat roles?

- ❑ During the World War II, the then Soviet Union employed thousands of women officers inside even the battle tanks.
- ❑ There are at least 25 countries, many of them advanced like the United States, Canada, Germany, Australia, South Africa, Israel and Russia, which formally permit women in combat positions. Even Pakistan allows women as fighter pilots.
- ❑ It is argued that the question of women being brutalised if captured cannot be overstretched (even though in many cases it is true) as today's women officers opting for combat roles know what their challenges are and they are prepared for all eventualities as long as they do not affect their resolve or the primary objective of overpowering the enemies.
- ❑ They are included in paramilitary forces (except Assam Rifles) which are also physically demanding in nature. Even BSF have an all women battalion to guard border.

Integrated Battle Groups

Recently, Indian Army has postponed the official launch of its new integrated battle groups (IBGs) because of the ongoing Covid-19 pandemic. IBGs are brigade-sized, agile, self-sufficient combat formations, which can swiftly launch strikes againstss adversary in case of hostilities. They will be able to mobilize within 12-48 hours based on the location. The integrated units for the border will be all-encompassing, with artillery, armoured, combat engineers and signal units. Currently, during hostilities a brigade has to wait to be augmented by different types of units which increase the time to mobilize. The IBGs are to perform both offensive roles, involving cross-border operations, and defensive roles to withstand an enemy attack. Each IBG would be tailor-made based on Threat, Terrain and Task and resources will be allotted based on the three Ts. They need to be light so they will be low on logistics.

Issues with Integrated Battle Groups

- ❑ China and Pakistan are both nuclear states. Pakistan as a policy has enunciated that it will use nuclear weapons the moment India threaten its green belt or its nuclear arsenals or if it feels that Pakistan is going to suffer major losses during a war.
- ❑ Therefore, it is important for India to not breach Pakistan's nuclear threshold during war. It is for this reason that the concept of IBG is being formulated.
- ❑ The various corps are equipped and organized to constitute 'strike corps' for offensive role and 'holding corps' to maintain territorial integrity of own international border.
- ❑ These units have a specific role while they are a part of a particular formation (strike/ holding) their roles vary with time and during operations, they are grouped together. Hence, their integration and synergy may fall short of the expectations

- ❑ Further, it was observed during OP Parakram, when India planned to launch an offensive into Pakistan after the terrorist attack on Parliament on 13 December 2001 that it took more than two weeks of time to mobilize and reorganize troops into battle groups for launching across the border.

Suggestions for Integrated Battle Groups

- ❑ IBGs are expected to be game changers that will alter the way the Indian Army strategises for wars.
- ❑ These specialised groups to ensure better integration and self-sufficiency as compared to the existing formations.
- ❑ During hostilities, the current system requires a brigade to wait to be augmented by various types of units, such as artillery and logistics, which raises its time to mobilise.
- ❑ This won't be the case with IBGs, which will be self-sufficient and inbuilt with all such units, and hence, easier to mobilise.
- ❑ This is one of the major reorganization plans of the Indian Army with the aim of enhancing command efficiency and the capacities for rapid response and coordinated operations.

GSSCORE

An Institute for Civil Services

GYAN CAPSULES

YOUR BOOSTER DOSE

**MAINS
ANSWER WRITING**



BHARAT KATHA



GOOD PRACTICE



Monthly
CURRENT AFFAIRS



Weekly
CURRENT AFFAIRS



**FREE MENTORSHIP
SESSION (FMS)**



DATA STORY



SCAN QR CODE TO REGISTER / DOWNLOAD



1B, Second Floor, Pusa Road, Karol Bagh,
New Delhi - 110005 (Beside Karol Bagh
Metro Station Gate No. 8)



8448496262



iasscore.in



SUCCESS IS A PRACTICE WE DO!

