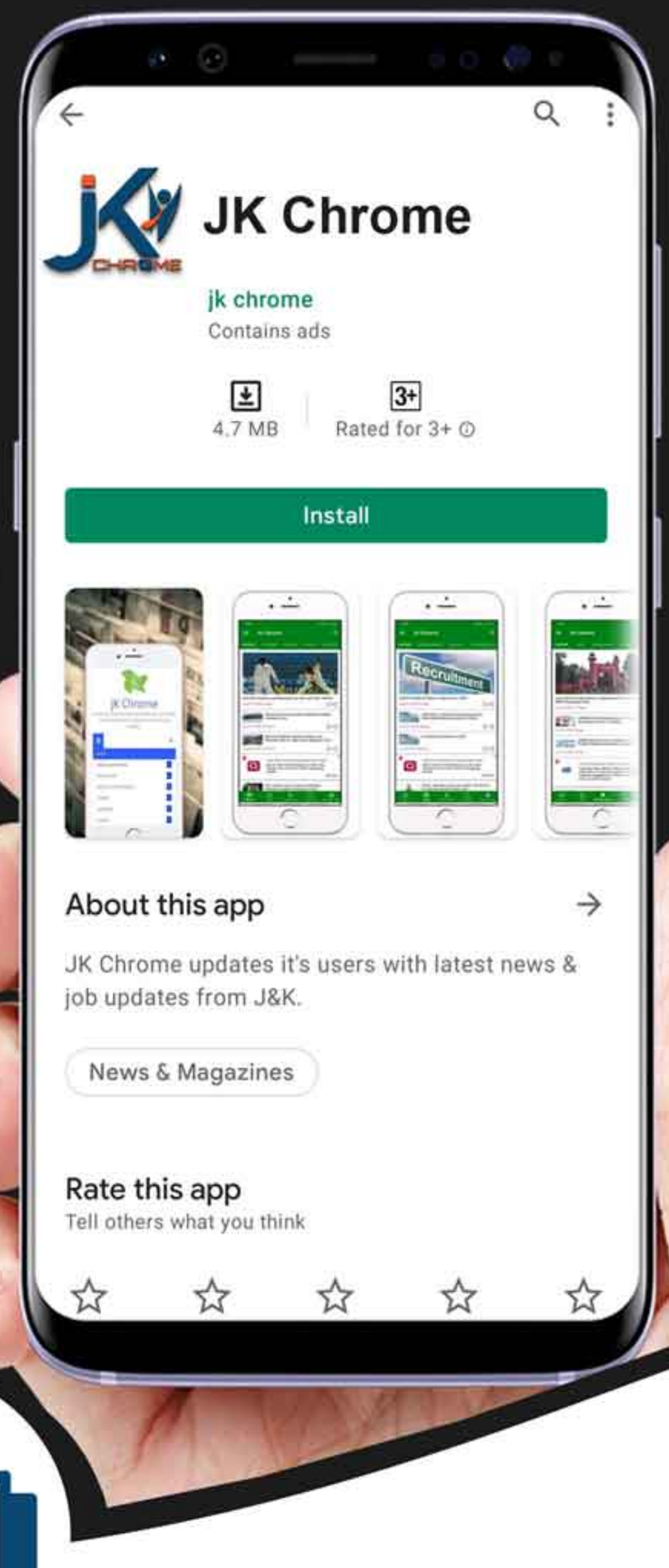
JK Chrome

JK Chrome | Employment Portal



Rated No.1 Job Application of India

Sarkari Naukri
Private Jobs
Employment News
Study Material
Notifications

JOBS

NOTIFICATIONS

G.K

STUDY MATERIAL

GET IT ON Google play

JK Chrome
jk chrome
Contains ads

Click here to DOWNLOAD

www.jkchrome.com | Email : contact@jkchrome.com

INTERNAL SECURITY

INDEX

Internal Security: An overview of Indian Scenario

1.1. INTRODUCTION

Security is the most fundamental interest of a nation-state. In its rudimentary form, security means protection from hostile forces, but if considered in its widest scope it can refer to developmental security, availability of essentials as in food and water security, security of borders, protection of critical infrastructure, economic interests, institutions and people. Considering a narrow definition, **National Security** is the protection of a nation-state, including its citizens, economy, and institutions, from harm. In the words of Harold Brown, former US Secretary of Defense – "National security… is the ability to preserve the nation's physical integrity and territory; to maintain its economic relations with the rest of the world on reasonable terms; to preserve its nature, institutions, and governance from disruption from outside; and to control its borders."

1.1.1. Threats to National Security

One of the earliest studies delineating the security threats faced by a state is **Kautilya's Arthashastra**. It classified threats faced by a state into four categories on the basis of origin of threats viz., internal, external, internally-aided external and externally-aided internal threats. As the nature of society, economy and government has become more complex in an interconnected and technologically advanced world, the threats to security have also evolved. Thus, apart from conventional threats from other states or challenge to authority from within, we have threats of terrorism, organized crimes, economic disruptions, disasters, threats to energy security, environment, scarcity of food and essentials, cyber-threats, pandemics etc.

In modern times, threats from **hostile nations** can manifest in form of direct confrontation between armed forces or actions performed through proxies. Hezbollah's threat towards Israel is an example of using proxy (by Iran) for achieving ends that may be difficult to harness directly. The threats to security from hostile nations can also involve indirect, subtle and harder to detect acts like election interference, espionage, fake currency circulation etc. **Proliferation** of weapons of mass destruction is a major associated threat to security of nations. Proliferation refers to development and stockpiling of advanced weapons by hostile nations. It creates a situation of **security dilemma,** distrust and projection of threats - real or imaginary, forcing other countries to engage in arms build-up for their safety. When China conducted nuclear test in 1964, it compelled India to explore use of atomic energy for military purposes. Situations of suspicion and lack of trust like these lead to arms race and increases militarization of nation-states, which pushes countries closer to the brink of war.

Terrorism is another category of modern security threats and can easily be counted among the biggest security challenges of our times. Terrorism is an act of violence which when done attempts to acquire or maintain power by intimidation, through inducing fear and helplessness in the minds of the people at large or any section thereof. The objectives and forms of terrorism may vary based on political, socio-economic and religious dimensions. Be it

the actions of Boko Haram in Nigeria, rise of ISIS or the lone wolf attacks that took inspiration from it, the world has witnessed a spurt of wide-ranging terrorist activities in recent years. Despite posing a grave threat to peace and tranquility, across the world, consensus on a universal definition for terrorism has yet not been achieved due to pursuit of narrow self-interests by countries in international relations.

With the advent of the internet, new dimensions of opportunities and threats have opened up in our world. **Cybercrimes** are among such newly emergent threats. These are acts that violate the laws of a nation using information and communication technology (ICT) to either target networks, systems, data, websites, steal technology and trade secrets or to facilitate any crime. Cybercrimes know no physical boundary and their operations are conducted with greater ease and greater speed as compared to traditional crimes. In a rapidly digitizing world, computer systems and electronic devices are performing many critical functions ranging from storing personal information of an individual to controlling critical infrastructure of a nation, which enhances the culpability to security threats from the cyber domain. In 2021, a ransomware cyber-attack crippled USA based company Colonial Pipeline's systems forcing it to halt its fuel supply operations across the company's country-wide network of oil pipelines.

Lastly, **Natural Disasters** constitute a hidden threat to security interests of a nation. The repercussions of natural disasters for national security are often not visible, till a disaster strikes

Threat to Country's Airspace

Airspace can be defined as the part of the sky that is above a country and that belongs to that country by law. Under the **Convention on International Civil Aviation** (the Chicago Convention), each state has complete and exclusive sovereignty over the airspace above its territory. In other words, a state is exclusively competent to exercise its legislative, administrative and judicial powers within its national airspace.

However, there have been incidents where some states/countries have taken steps disrupting the stability and **violating sovereignty of other countries** over their air space. In this light the most controversial activities have been declaration of **Air Defense Identification Zones** (ADIZ). ADIZ is airspace over land or water in which a country identifies, locates, and controls/directs civil aircraft in the interest of its national security. These zones may extend beyond a country's territory to give the country more time to respond to possible hostile activities. The first ADIZ was established by the United States during the Korean war. At present, about 20 odd countries, including India, China, Pakistan etc., have such zones.

In November, 2013 the People's Republic of China (PRC) established a zone in the East China Sea. The act of China drew opposition from China's East and Southeast Asian neighbors as well as EU and USA. The reason for criticism from various quarter was that China's ADIZ in the East China Sea covered the **airspace over Japanese-controlled Senkaku Islands** (known as Diaoyu Islands in China). Also, Chinese ADIZ covered **airspace over Socotra Rock,** which is claimed by South Korea. Another matter of concern was that China's ADIZ overlapped with the ADIZ of few other countries. Thus, violation of sovereignty over a country's airspace, through direct or indirect means, is an existing challenge which has the potential to disrupt international peace and stability. As such incidents can lead to **escalation of disputes** and regional conflict, there is a need to take corrective steps. In this light, all parties need to make/respect their commitments to international rules-based order. Further, all states should display mutual respect for each other's sovereignty. Lastly, any dispute or conflict should be handled peacefully by employing political and diplomatic means.

Q. International civil aviation laws provide all countries complete and exclusive sovereignty over the airspace above their territory. What do you understand by 'airspace' What are the implications of these laws on the space above this airspace? Discuss the challenges which this poses and suggest ways to contain the threat. **(UPSC 2014)**

Pandemic and National Security

Covid-19 highlighted the comprehensive threat that **biological disasters** can pose to security. While the origin of the pandemic and it being a man-made or natural disaster remain debatable, the challenge to security from pandemic in countries across the world was for everyone to see. In response, nations resorted to conventional measures for security like border controls and exercise of authority over social and economic activities. This has resulted in making the state very visible and in-the-face of citizens while trying to grapple with the immensely complex challenge the pandemic has posed to public safety and security. Along with the security threats created by Covid-19, the global disruption in economies, **threats to livelihood**, forced measures for lockdowns, disease surveillance etc. overwhelmed societies as the pandemic kept on expanding. We saw protests and clashes between security apparatus and the people, incidents of communalization, perpetration of racial stereotypes and discrimination. All these factors constitute conventional threats to security and public safety. The stark security situation was compounded by **incursions across the India-China border** by the Chinese army. For a time, it was feared that infection among Indian soldiers could paralyze their ability to secure borders and handle a hostile neighbor as is known from historical examples about the role of plagues in success of Mongols in eastern Europe or of Europeans in Americas.

and causes large damage to life, property, economy, infrastructure and disrupts the flow of social life in one big swoop. Natural disasters can derail hard earned gains of socio-economic development. It can be among the reasons for alienation and hostility of people towards state, erosion of authority and cultivation of anarchy and lawlessness. Catastrophes exacerbate pre-existing problems and inequalities as vulnerable population are disproportionately affected. In addition, threats like **climate change** are projected to lead towards inundation of small islands threatening the very existence of many Island nations. Submergence of coastal areas would force large scale migration in countries like Bangladesh which have dense population density in coastal regions. Situations of climate refugees moving across borders has potential to threaten regional peace, invoke insurgencies and may lead to international conflicts and war.

The various categories of threats to security as discussed above can act in solitude or in combination to pose a more complex threat to a nation. For example, Pakistan, for long, had been trying to incite unrest in Kashmir, but militancy did not start to gain significant ground in the valley till late-1980s. Stoking the fire of militancy in the region required concurrence of international factors like Soviet withdrawal from Afghanistan, western-support of Pakistan, rising wave of Islamism within neighboring Pakistan, and local misgivings about rumored election rigging.

1.2. INTERNAL SECURITY

Generally, threats to security can be briefly differentiated into internal and external security. Internal security is the domain that deal with maintaining **peace within the borders** of a sovereign nation by effectively countering the threats to internal security. It pertains to upholding the sovereignty of the nation within its territorial boundaries. In contrast, external security is concerned with upholding sovereignty, independence and territorial integrity from military-aided threats of another country. It is the sole responsibility of armed forces of the country under Ministry of Defence. Responsibility for ensuring internal security could lie with police, paramilitary forces, and sometimes with the military.

Threats to internal security may be directed towards citizens or against the state's administrative and security machinery. The Internal security threats can manifest themselves in various forms ranging from organized crimes to insurgencies and movement for secession. Thus, in addressing internal security challenges, the state has wide obligations involving prevention of crimes, protecting fundamental rights of its citizens, assuring citizens' life, property and social security and averting challenges to territorial integrity of the nation. The primary responsibility in maintenance of internal security lies with the police which can be supported by paramilitary forces in times of need. The subject matter of internal security comes under

the purview of Ministry of Home Affairs (MHA) in India, which also manages the paramilitary forces and their deployment in controlling various internal security challenges as and when needed.

1.2.1. Dimensions of Internal Security

Now that we know what internal security essentially means, it's time to expand on that understanding through elaboration on various dimensions of internal security. **Physical security** provisions by the state constitute a major element of internal security. It upholds national sovereignty within the borders by asserting the authority of the state. It involves maintaining law & order so that citizens have the possibility to develop themselves in situations of peace, and achieve their aspirations making the best use of their potential. **Energy security** is essential to keep the wheels of the national economy running. In era of globalization, disruption in a country's energy and fuel supplies can create domestic unrest through high inflation, unemployment, trade disruption and flight of foreign capital. Such threats can affect domestic politics, create protest movements and trigger regime change through undue foreign influence. **Economic security** refers to an ability to maintain decent standard of living, resist external disruptions to economy and protecting the economic interests of various sections of society. It covers aspects like threats of economic sanctions, overdependence on imports particularly from a single country, lack of sectoral diversity in national economy such as oil-based economies, **food insecurity**, vulnerability to balance of payment crisis etc. Economic security is not very dissimilar to energy security in terms of its implications.

Increasingly, the description of Internal security is shifting away from a state-centric understanding to human-centric perspectives on security. Accordingly, new dimensions have been added to internal security. Thus **development, ecology and identity** have become essential in understanding internal security and reducing conflicts. In upholding rule of law, one should not be unmindful of the principle of equity inherent in principle of 'equality before law' and 'equal protection of law'. Local ownership of resources and development of local governance institutions is necessary to bring people on-board. Measures like protection of forest groves and respect for traditional rights of forest dwelling communities, their way of life, identities and customs ensure that no section of society feels alienated. Internal security is a holistic concept which incorporate all of the above dimensions having direct or indirect implications for upholding national sovereignty within the territorial limits of the country.

1.2.2. Conventional and Non-Conventional Challenges to Internal Security

The **conventional challenges** to internal security are those that directly challenge the authority of the state. Terrorism, organized crimes and volatile neighborhood are main sources of such threats. **Terrorism** has emerged as a global threat to peace. It affects developing as well as the developed world. Various factions of terrorists have emerged with different demands but their motives remain same i.e., to advance their political ends by inducing fear and intimidation as they cause damage to life and property of innocent people. **Organized crime** acts as a source of illegality, as they flout the law of the land to create a shadow economy that hollows out the nation of its resources. Violence, corruption, anarchy, linkages with terrorism and secessionist movements are some other worrying aspects of organized crime. Organized crime is also seen to evolve into system of parallel policing, making state defunct in many areas in providing security to citizens. **Instability in neighborhood** undermines the sovereignty of the country in numerous ways. The neighborhood becomes a source of infiltration of illegal immigrants, breeding ground of anarchist elements, transit routes for smuggling and safe-havens for insurgents.

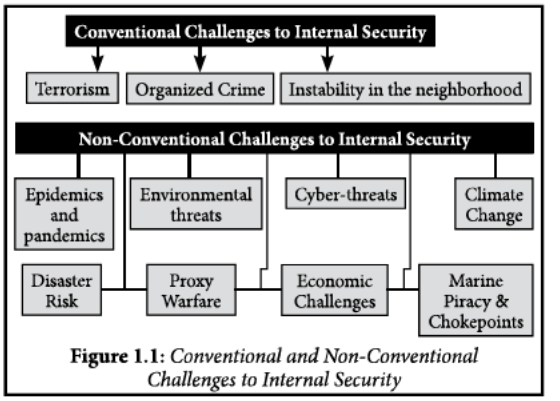


Figure 1.1: *Conventional and Non-Conventional Challenges to Internal Security*

Apart from these conventional challenges, a number of **non-conventional challenges** threaten internal security and put excessive strain on the security apparatus of the country. Use of proxies against hostile countries has become the new instrument of invisible warfare. Often these threats create situations of civil war. The reason for using **proxy warfare** is that inter-state wars are no more preferable due to large political and economic costs involved in them. But even proxy warfare is becoming ineffective instruments for countries in securing their political or economic interests as seen in the rise of ISIS from Syrian civil war. **Economic sanctions** are used sometimes as alternative tactic, which pose **economic challenge** to internal security of the target countries, often with hope of regime change, and in this process undermining their sovereignty. The globally inter-dependent economies are also vulnerable to unforeseen events in distant countries. For example, the breakout of Covid-19 **pandemic** from China and over-dependence of global economy on Chinese goods resulted in debilitating circumstance such as shortage of APIs to produce medicines. The vulnerabilities of global sea lanes of transportation to **maritime piracy** and closure of maritime chokepoints exacerbate the economic vulnerabilities of the nations and threaten their internal security.

Cyber-threats take advantage of increasing dependence of the world on information and communication technologies (ICT) which makes a range of government bodies, administrative systems, security apparatus, businesses and private citizens potential targets of cyber-crimes viz, phishing, hacking, spyware, ransomware, honey-trapping, **denial-of-service attacks** etc. Moreover, use of social media platforms by terrorist organisations for radicalization and recruitment are also direct threats to internal security. Dark-web is a hell-hole of criminal activities that operate beyond the pale of law enforcement authorities.

Threats to natural environment and environment destruction due to unabated materialism and quest for economic development have put communities in conflict with each other and with state and large corporate organizations. Cultivation of water-intensive crops like paddy in north-west India has created situation of water distress, inter- state river-water conflicts like Sutlej -Yamuna Link canal and Cauvery River water dispute and chronic problem of air pollution due to stubble-burning are some of the socio-political and environmental threats. Exorbitant amount of greenhouse gases emitted since the start of Industrial Revolution in 18th century created the problem of global warming and **climate change**. Effects like rapidly melting glaciers, erratic weather patterns, increasing frequency of natural disasters like cyclone, storm surge etc. are already being witnessed. Problems like desertification and submergence of coast are likely to displace crores of people. The effects of climate change and increasing **disaster risks** are likely to be borne by the downtrodden sections of societies resulting in climate refugees and situations of conflicts are expected to arise due to the above number of factors.

1.3. INDIA'S INTERNAL SECURITY CHALLENGES

India faces a mix of both conventional and non-conventional challenges to its internal security. **Left-Wing Extremism**, also known as Naxalism or Maoism is considered to be the most important and among the oldest internal security concerns in the country. The ultimate goal of Maoism to achieve a stateless society, and for that end it seeks to wage a 'people's war' by putting the people particularly the downtrodden sections of society in direct confrontation with the state. Their methodology of attacking state's symbols like police, schools and other government institutions creates a law & order situation. Also, their inclination towards violence against symbols of state intimidates other citizens and has resulted in several tribal areas getting disconnected from the national mainstream. Late 1980s saw the advent of militancy in **Kashmir** which resulted in large scale migration of Kashmiri Pandits. Pakistan used the Kashmir issue to wage cross-border terrorism through state-sponsored and trained groups. The support from Pakistan also led to development of homegrown terrorist groups like SIMI, Indian Mujahideen, etc. which were largely ideologically and financially supported and trained by Pakistan-based terrorist groups. **Northeast** India is mainly a tribal society with wide ethnic diversity. A centralized system of governance

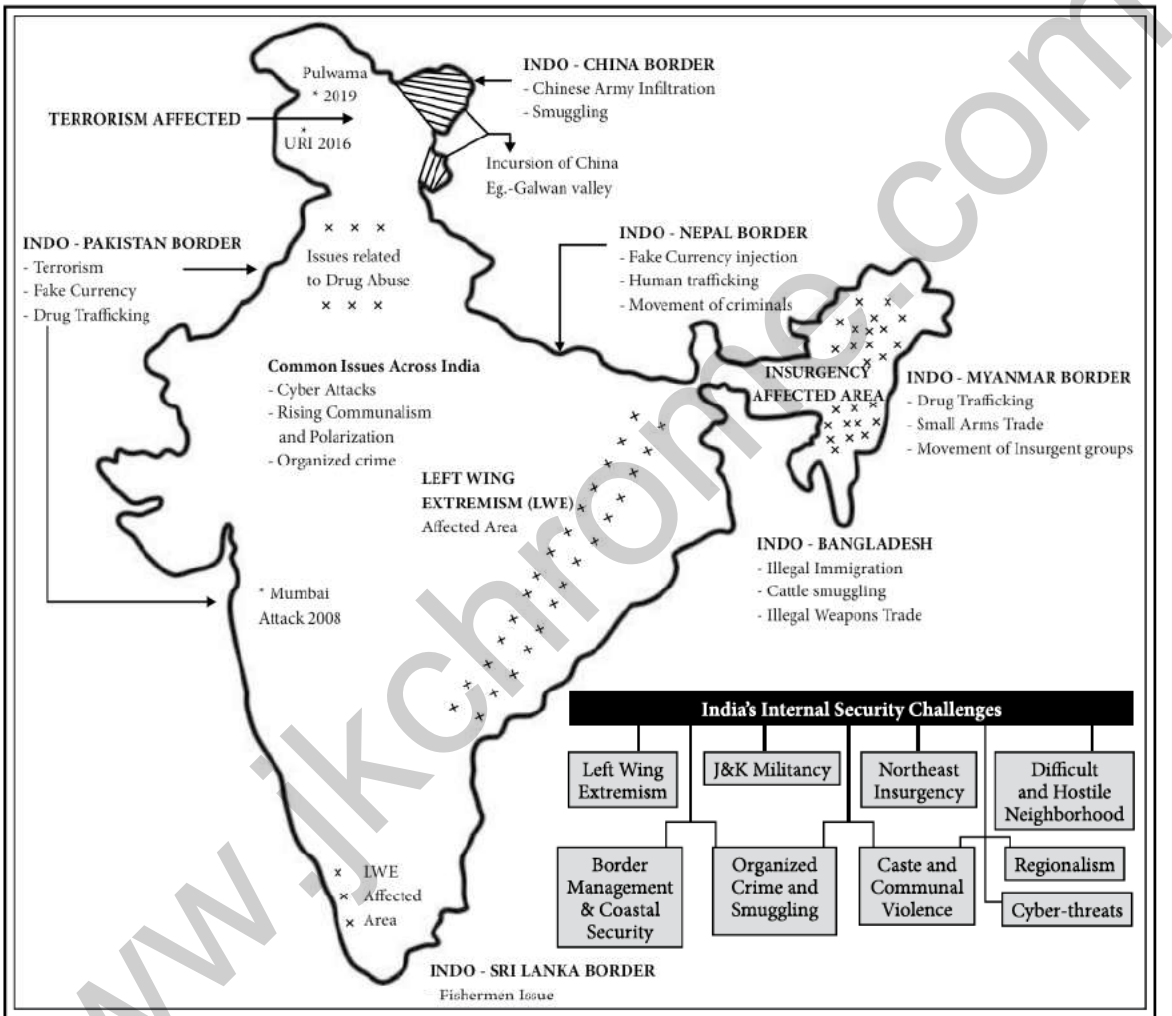


Figure 1.2: *India's Internal Security Challenges*

after independence was not very responsive and suited to locals' aspirations and the diverse ways, customs and rituals of tribal life. Disgruntled locals, supported by China and what was earlier East Pakistan, rose up in arms against the Indian state. This insurgency has affected 7 of the northeast states with each insurgent groups having varying motives and demands.

A **difficult and hostile neighborhood** has been a bane for India's internal security. While Pakistan's cultivation of terrorist groups against India caused direct emergence of a number of internal security threats, insurgencies in north-east also utilize the factor of a difficult terrain and porous borders between India-Bangladesh and India-Myanmar to their advantage, to evade actions by security forces. India's proximity to the golden triangle in the east and the golden crescent in the west makes it a transit route for the illegal **international drug trade**. Recent upheaval in Afghanistan due to abrupt withdrawal of US forces has left the region in a civil war situation and a breeding ground for terrorism. In Myanmar, the issue of Rohingyas and the military coup have catalyzed flow of people across the border, breaching India's territorial sovereignty. Such issues pose problems in **border management** as well, which along with **coastal security** is another core aspect of internal security. India has a vast coastline and land boundary which runs through a diverse and difficult terrain making border management a herculean task with direct repercussion for emergence of security threats in

the country. The 26/11 attacks in Mumbai in 2008, for example, were possible because of a breach in India's coastal security. Militancy in Kashmir is supported by Pakistan through infiltration of terrorists across the Line of Control.

The threats of communalism loom large in present India. Origin of **communalism** lie in the 'Divide and Rule' policy of British India, which resulted in the lamentable partition of India in 1947. But these thorns of hatred have continued to scar the Indian psyche through the decades after independence. The Nellie massacre 1983, Anti-Sikh riots 1984, Babri Masjid Riots 1992-93, Gujarat riots 2002, Muzaffarnagar riots 2013 etc. are some of the examples. Also, India - with its large diversity - has witnessed **caste, ethnic and regional conflicts**. The anti-Hindu riots of the 1950s and 60s, 2008 attacks on migrants in Maharashtra, numerous incidents of caste atrocities, northeast insurgencies based on ethnicity are notable examples. Presence of gross inequalities fueled by poor economic opportunities makes different caste and ethnic groups antagonistic to each other in their competition to grab the small pie of development and resources. The conflicts are also conflated by short-sighted politics and foreign influences who are ever willing to fish in troubled waters to perturb internal security in India.

The diverse nature of India's **multi-religious** and **multi-ethnic** society makes it vulnerable to the impacts of radicalization. Radicalization is the social and psychological process of commitment to extremist political or religious ideology. Radicalization is a serious internal security challenge. It keeps the overall environment of the nation charged and thus unstable. It increases the vulnerability for communal riots and lone wolf terrorist attacks. It creates a sense of alienation among the people which results in their taking extreme and violent steps. It leads to extremism and thus disturbs the peace and harmony in society. These radicals adopt extreme political, social or religious ideals and aspirations that often results in communal riots, mob lynching etc. If opportunity presents radicalized sections may not hesitate to perpetrate violence.

Multiplicities of identities, ethnicities, races etc., are often the cause of not only internal instability but also that of ensuing external threats. The role of identity/ethnicity in creating challenges for internal security was witnessed in the **Balkan wars** as well as during the disintegration of the Soviet empire. In our immediate neighborhood too, ethnicity/ religious identity has been an important factor in determining the geo-politics of the region. Formation of Bangladesh, which was previously East Pakistan, in 1971 had religious and ethnic undertone. Also, the civil war in Sri-Lanka between the Sinhalese and the Ethnic-Tamils had its origin in ethnic dispute between the two. Conflicts with ethnic-linguistic minority Rohingyas in Myanmar have given rise to militant movements through groups like the Arakan army. In Nepal, there are ethnic tensions between the hill people and Madhesi. Many of the ethnic conflicts in north-east have been accommodated through a mixture of constitutional flexibility and administrative innovation in form of measures like territorial councils. Political sagacity nipped the linguistic conflicts in their bud in 1950s. Sectarian violence has been absent for the societal reasons as well as for the fact that people of the country chose and continue to comply with a plural, secular framework as opposed to an ethnic or religious basis of their state and society as in countries like Pakistan, Myanmar, Sri Lanka, Bangladesh etc.

Although India is relatively immune to the ethnic and religious conflicts which prevail in its neighborhood, there are reasons which can act as catalyst for absorption of such influences which might pose a **challenge to Internal Security situation** in India. Religious diversity can be targeted to cultivate extremism and strife. Communal riots like the Anti-Sikh riots, Godhra riots, Saharanpur riots etc. lead to mutual hatred making individuals from different communities prone to radicalization. Presence of extremist organizations like pro- Khalistan groups, ULFA, Naxal organizations, Indian Mujahideen are cause of worry. Movements like Tablighi Jamaat have influence which cuts across nationalities. Pakistan's proxy war has been a source of propaganda and radicalization in Kashmir for decades. Infiltrators from Pakistan radicalize the youth in the valley fueling separatist sentiments against India. Burhan Wani, a 21-year-old Kashmiri boy is an example how the young people are prone to be radicalized. Social media is increasingly becoming a tool for

transmission of radical influences. Because of its foundational cosmopolitan nature, real or fake incidents of persecution in one part of the world arouse feelings of **co-religionists and ethnicities** across international borders. There have been several instances where videos of violence and destruction of religious places in other countries are passed off as evidence of persecution and strife within country, which ends up feeding radicalization. At times this translates into violence.

Lastly, **politics of polarization** divides society to secure votes. The short-term gains end up cultivating long-lasting mutual hatred among people, thus, creating a potential target for radicalization and opening up long-healed wounds that define the international borders of the region.

In such situation, de-radicalization requires counter-messaging campaigns that help reframe the narrative of conflict wherever it prevails. To reach the right audience, social media can be an aid. For example, **Operation Chakravyuh** was launched by IB to communicate with Indian youths who intended to join the IS outfit. UNSECO's efforts on 'Preventing Violent Extremism' must be pushed. International experiences can be a source of learning, such as the Indonesian de-radicalization drive, or Nigeria's Deradicalization, Rehabilitation, and Reintegration (DRR) programs to counter Boko Haram. SMART policing model of Andhra Pradesh could be replicated across the country to ensure a pro-active approach and nipping radicalizing efforts in the bud.

For years India's plurality has absorbed within itself - different ideologies and viewpoints. It has provided space for numerous streams of social sects and varied political notions to co-exist and grow. Therefore, besides reactive containment of radicalization and its fallouts through improved policing, intelligence-based responses and application of legal deterrence, there is also a need to address the very causes of alienation through socio-cultural attitudes of assimilation.

Q. "The diverse nature of India as a multi-religious and multi-ethnic society is not immune to the impact of radicalism which is seen in her neighbourhood? Discuss along with strategies to be adopted to counter this environment. **(UPSC 2014)**

Another significant threat to India's internal security is associated with the incidents of mob violence and lynching. Mob lynching is an act of premeditated extrajudicial killing by a group of people, often targeted against a particular individual or group. Mob lynching is based on some false information, unconfirmed rumours etc. Act of lynching leads to mockery of law and order. Recently, mob-lynching incidents have increased in India due to various reasons. The lynching of Pehlu Khan in Rajasthan (lynched by Gau Rakshaks), Mohammad Akhlaq in Dadri (on suspicion of cow slaughter), Farooque Khan in Imphal (on suspicion of vehicle theft), lynching of a monk by tribals in Palghar etc., are a few of many such incidents. There are several factors behind the spurt in lynching/mob violence incidents in the country. Analysts opine that the foremost factor is the **failure of state.** People are losing their faith in law-and-order machinery therefore they are taking laws in their hand. Further, there is a tangible **rise in the level of intolerance.** According to some experts, intolerance especially against marginalised has increased in recent times. For example, protection of religious symbols/animals is often used as a pretext to commit mob lynching. In this light the activities of cow vigilantes are of particular concern. On several counts the cow vigilantes held law and order hostage by lynching the people of a particular minority community. In 2017, three Muslim youths were mercilessly lynched in Durgapur, by a mob of cow vigilantes over a suspicion of cow theft.

With rise in anger fuelled by fake news and propagandas, mob lynching cases have shown a definitive increase. Yet another cause of mob violence is to do with a rise in unemployment. Unemployed youth are being **misguided ideologically** by politicians and religious groups. As a result, the gullible youth act against certain sects in a way that is inimical to not only law and order but also to the social harmony. Further, a sense of insecurity, which in itself is a result of social disharmony, becomes a cause for incidents of mob violence. Mob violence may be done for defence against any perceived and presumed threat from other social groups. Such threats are often misplaced and are a propaganda of the hate mongers. Also, a negative attitude or bias against any group due to historical or social reasons may

motivate mob to commit a hate crime. For example, Muslim being tagged as terrorist lead to acts of lynching against them by the mob.

In addition, **mob mentality** is a major factor behind the rise in mob lynching/mob violence. When people act in a mob, the law-and-order agencies find it difficult to take action against them. As the mob is faceless, it **enthuses people with impunity** to act in a lawless manner. Dhule lynching incident is a case in point. In Dhule, mob violence fanned by child-abduction rumours snuffed out five lives, thus making a mockery of the law-and-order situation in the region. Further, the laws to deal with lynching are not implemented in a sound manner and there is tangible political pressure on the government agencies to hush the matter under the carpet. The political leaders are believed to be acting in a communal way keeping their **myopic political gains** in mind. Also, there is a sense of diffused responsibility in the preparators of mob violence, wherein individual responsibility is undermined. Further, the social media, fake news and political propaganda create a dangerous cocktail which can instigate a mob violence in the blink of an eye, with giving the law-and-order agencies time to react or prepare. Mob violence is also derogatory in its effect, as it dehumanizes the victim.

Incidents of mob violence are not only a threat to the law-and-order situation of the country but are also detrimental to the **communal and social harmony** of the region. Mob-violence often have a sectarian dimension involved. Cleavages along religious or caste lines are reinforced/aggravated by the incidents of mob violence. What is more problematic is the after effects of such incidents. Mob violence/lynching incidents tend to repeat themselves. Hence, if such incident occurs once in any region, it is likely that the region may become prone to such incidents in the future. Mob-violence puts tremendous strain upon the law-and-order machinery of the country. Already starved of the vital human resource, the law-and-order machinery gets drained of its time as well as personnel in order to deal with incidents of mob violence. This in turn affects other duties and task of the enforcement agencies.

Mob violence is regressive in a way that it destroys the precious public resources/properties in its wake. The **anonymity of the mob** allows it to act with a sense of impunity. Social infrastructure like government offices, vehicles, hospitals, public places, utilities etc., are first to be targeted by the mob. Further, private properties in form of shops, houses etc., are also affected by the violent activities of the mob. In addition, mob violence has the negative effect of disrupting the peaceful day to day life. It affects the office goers, children, business persons etc., thus in a way affecting normal life. Another chilling effect of mob violence/lynching is the fear and insecurity it causes upon the targeted group. The target group is mostly the minority community, marginalised sections, or people from the so-called lower castes. When any group/individual is made a victim of mob violence/lynching, it generates a sense of alienation in them. Also, mob violence goes against the ethos of our constitution. It deprives a group or an individual of their dignity and also causes an irreversible damage to the **spirit of fraternity and brotherhood.**

Given the enormity of the problem there is a need to take consolidated actions in order to check the incidents of mob-violence/lynching. In spate of lynching incidents happening in the country a need is felt to bring in a suitable legislation to deal with the menace of mob violence. The proposed law should clearly define the terms associated with the crime viz. lynching, mob and victim. It should make lynching a non-bailable offence, criminalise failure of duty by police officers, designate judges for trial, define compensation and rehabilitation for victims and witnesses within a definite time frame. In addition, there is a need to reform the electoral as well as political ecosystem. Political leaders should incorporate a **broad, inclusive and non-communal vision** for the society. Further, the lynching cases should be tried by fast-track courts with day-to-day hearings. It is important to punish the culprit with stringent punishment and conclusion of the cases within 6 months. In addition, community should be sensitised towards the rights of other citizens and danger of mob crimes for social cohesion. Awareness campaigns are needed to sensitise people about the plight of others.

Also, community should be engaged in order to nip in the bud any attempts to disrupt the communal harmony. By fostering partnerships with the community state can enable communities

and law enforcement to work together to prevent and respond to hate crimes. Helpline should be established for reporting of mob lynching. Further, there is a need for youth involvement and counselling. The majority of act of lynching are committed by persons who are below 30 years. Youth are also often more vulnerable to violent attacks, bullying, and other forms of harassment. To combat this teachers and school administrators should educate their students and staff on the nature of such incidents and crimes and how to prevent them. Also, police should train new recruits and existing officers and deputies on mob lynching and other related issues. It shall be the duty of every police officer to cause a mob to disperse, which, in his/her opinion, has a **propensity to cause violence** in the disguise of vigilantism or otherwise. 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. Central and the state governments should make use of the **broadcasts on radio and television** and other media platforms for generating awareness among the citizens. These platforms can be used as tools for spreading communal harmony and brotherhood.

Few states like Rajasthan, West Bengal, Jharkhand and Manipur have passed state specific laws which criminalises mob lynching. However, in case of all the four states the bills are pending and await the President's nod as some punishments laid down in the bills were higher than those in the central statutes. In such scenario, t he President has to go with the advice given by the Council of Ministers, represented by the Ministry of Home Affairs (MHA). The MHA examines the state legislations on three grounds, viz. repugnancy with central laws, deviation from national or central policy, legal and constitutional validity. Further, in 2018, the Supreme Court asked Parliament to make lynching a separate offence. However, the MHA has informed the parliament that the government has decided to overhaul the IPC and the CrPC and mob-lynching would also be examined by the committee.

Q. Mob violence is emerging as a serious law and order problem in India. By giving suitable examples, analyze the causes and consequences of such violence.
(UPSC 2017)

Cyber security is the among recent additions to India's long list of internal security challenges. Given the rapid growth of digitalization in the country, many a systems and services in government and private businesses have become dependent on digital services. People's lives are unimaginable without smartphones and social media. The dependence on digital medium has opened up vulnerabilities to cyber-threats and digital scams. Phenomena like the rise of Jamtara, a small town in Jharkhand, as hub for cyber-crime is an instructive example of misuse of digital tools by people with limited outlets for their aspiration. Social media platforms are used to spread hatred, disinformation which ultimately culminates into violence. India has also witnessed increased cyber-attacks on its critical infrastructure by state and non-state actors.

1.3.1. Factors Responsible for Internal Security Problems

The different challenges for internal security problems in general or in context of India have some underlying factors which are fundamental in nature. A number of internal threats to internal security from organized crimes to terrorism and Naxalism can be attributed to **poverty and unemployment.** A legacy of colonial India, poverty and socio-economic backwardness is the primary reason for origin and spread of Maoism in India. Similarly, **governance deficit** is a significant factor influencing internal disturbance. Defunct governance widens the gap of already existing **socio-economic inequalities**. Frustrated with government's lethargy, administrative apathy and social marginalization, citizens may be forced to form an anti-state attitude. Poor governance is also at the root of **corruption**, which brews its own set of problems. It facilitates the rise of many threats to internal security including social alienation due to inefficiencies in the government system and facilitation of organized crimes and terrorism. India is infamous for its slow judicial processes and **delayed delivery of justice**. There is large pendency

of cases in courts. This leads to perpetrators of criminal acts going relatively unpunished and a culture of strongman politics, perpetuating the old **feudalism**. In parallel, we have huge number of socio-economically poor undertrials being put in jails and denied bails. Thus, lofty constitutional principles like equality, rule of law and rights are absent from day-to-day life of the marginalized sections, making them susceptible to influence from anti-state ideologies and criminal networks.

Caste is at the root of socio-economic inequalities in India. It divides society into groups, and restricts their social and economic mobility by putting barriers in access to opportunities. Caste-based divisions in society are detrimental to unity and integrity of the nation. Similarly, **communal tensions** fuel the feeling of constant contestation between communities based on religious identities. Communalism undermines the notion of civic nationalism and national fraternity based on constitutional ethos. Lingering communal tension along with poverty and inequality proves a fertile ground for mischief by radical forces and hostile countries. Terrorism and riots grow out of this problem. Also, India's geographical location, while historically a reason of prosperity, makes it susceptible to unique threats of smuggling of drugs, human trafficking, refugee influx etc. due to an **unstable neighborhood** from Afghanistan(west) to Myanmar(east).

1.3.2. Principles of India's Defence And Security Policy

The defence and security policy is the broader set of guidelines nation follows while dealing with any threat situation. The principles guiding the defence and security policy are guided by country's strategic objectives. India believes in the concept of "**Vasudhaiva Kutumbakam**", the firm conviction that the entire world is one family. Since ancient times and presently, as the world's largest democracy, India has no zest for conquest and territorial expansion. It poses no threat to other countries. As a believer of the principle of **Panchsheel**, India is opposed to interference in other countries' internal affairs and detests external interference in India's internal matters. India is traditionally opposed to systems of alliances between countries. A natural outcome of this outlook has been India's leadership of non-aligned movement (NAM) in the past and the desire for **strategic autonomy**, while cooperating with like-minded countries. This is clearly visible by India's logistic agreement with countries like USA and Russia. India's democratic traditions are reflected in its preference for dialogues and negotiation to settle disputes as seen in its handling of insurgencies.

At the same time, resort to force has been adopted for asserting the authority of the state and in effectively handling the grave exigencies of the times. For example, **Armed Forces Special Powers Act** 1958, or provision within IPC to deal with threat to public order, sedition, offences relating to religion etc. use colonial era authoritarian measures. Laws such as Unlawful Activities Prevention Act 1967, National Security Act 1980 and a number of public safety acts by state governments have provided additional measures to the government in countering internal security threats with the element of force. The system of constitutional rights and institutional division of power among branches of government creates a **system of checks and balances** against misuse of authority by the government in name of threats to national security.

India's defence and security policies are aimed at safeguarding the nation against the threat of conventional and non-conventional threats. Protecting citizens from impending threats originating either from inside or outside the country, securing public and private properties from destruction caused by anti-national forces, and constructively engaging with other nations towards common interests of a safe and secure world are its goals. Guided by Ashoka's policy of Dhamma, India is opposed to policy of conquest, but at same time, it has a strong will to resist domination and resist attempts at subverting national sovereignty.

Naxalism: Linkages Between Development & Spread of Extremism

2.1. INTRODUCTION

The former PM of India, Manmohan Singh, in his one of the speeches in 2006 and later too, called Left Wing Extremism (or Naxalism) as the **greatest internal security threat**. Left Wing Extremism or Naxalism refers to the **armed conflict** between the **far-left radical** communists and the Government of India. Naxalites favour **overthrow** of established **government** and replacing it with Leninist-Marxist kind of social system. According to the government data, over the past few decades, the LWE movement is suspected to have impacted 40 percent of India's territory and 35 percent of its population.

This movement started in 1969, under the leadership of **Charu Mazumdar, Kanu Sanyal** and **Jangal Santhal.** The left-wing extremists follow the **ideology of Mao Zedong** and believe that the solution of economic and political discrimination is violent overthrow of the government by the guerilla groups. The goal of the extremists is to implement their own vision of the State through 'revolution' and they did so by enlisting the support of the deprived and exploited sections of society residing in remote rural regions. The left-wing extremists are against the democratic principles and the developmental works undertaken in the remote regions. These developments are looked upon by the Maoists as potential threats to their very existence and their outdated ideology. The Maoists also destroy infrastructure like roads and telecom network to keep populations isolated from mainstream India.

2.1.1. Background

Left wing extremism or Naxalism, as commonly known in India, has its roots in **communist movements** which started after getting inspiration from the Great October revolution of Russia. The communist movements were started with an objective to end the capitalist colonial oppression in India. The communist movement gained momentum in India specially after the **Telangana struggle.**

The Telangana struggle started in 1946 by peasants against oppression of feudal lords, illegal taxations and forced evictions. The ideology spread to thousands of villages under the influence of Andhra MahaSabha and the Telangana struggle became the largest armed peasant uprising against the rent seeking landlords. By the end of 1947, communists were able to organize parallel administration in the form of village republics in 4000 villages. A group of volunteers called 'Dalam' was raised to fight Razakars and the police. But the movement weakened when Indian Army under 'police action' entered Hyderabad to fight the Nizam and Razakars. The Dalams were no match to the trained strength of the army and they retreated to forests. The movement fizzled out as the unity and strength got disrupted as the area came under government control.

2.2. ORIGIN OF NAXALISM OR LWE

The exploitation of tribals and poor people residing in resource rich regions was a regular phenomenon in colonial rule and it continued as a colonial legacy even after Independence.

An incident occurred in **Naxalbari,** a village in Darjeeling district of West Bengal (hence the term Naxalism) where on 2nd March 1967, a tribal youth Bimal Kesan, after obtaining a court order against his landlord Iswar Tirkey (a member of Bangla Congress), went to plough his field. He was stopped by the goons of the landlord. He went to seek help of Kanu Sanyal of Krishak Sabha who agreed to help him. The peasants occupied Iswar Tirkey's land, and he was forced to seek police action against them. Clashes took place between the police and the peasants who were led by **Charu Majumdar and Kanu Sanyal.** In the next few months, the movement spread to other states like Orissa, Andhra Pradesh, Tamil Nadu, Kerala and Uttar Pradesh. This extremist movement came to be called Naxalism and the extremists got the name Naxalites. They claim to follow the far-left radical communist ideology of Mao Zedong and call themselves 'Communist Revolutionaries'.

Maoism: Maoism is a form of communism developed by Mao Tse Tung. It is a doctrine to capture State power through a combination of armed insurgency, mass mobilization and strategic alliances. Follower of maoism also use propaganda and disinformation against State institutions. Mao called this process, the 'Protracted Peoples War', where the emphasis is on 'military line' to capture power. The central theme of Maoist ideology is the use of violence and armed insurrection as a means to capture State power. The Maoist ideology glorifies violence and the 'Peoples Liberation Guerrilla Army' (PLGA) cadres are trained specifically in the worst forms of violence to evoke terror among the population under their domination.

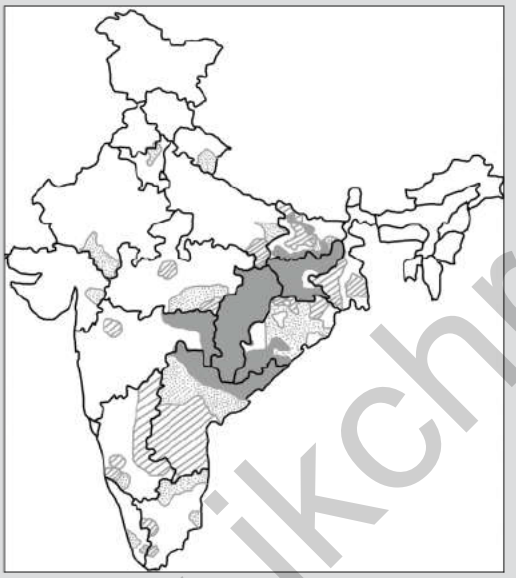
2.3. EVOLUTION OF LEFT-WING EXTREMISM

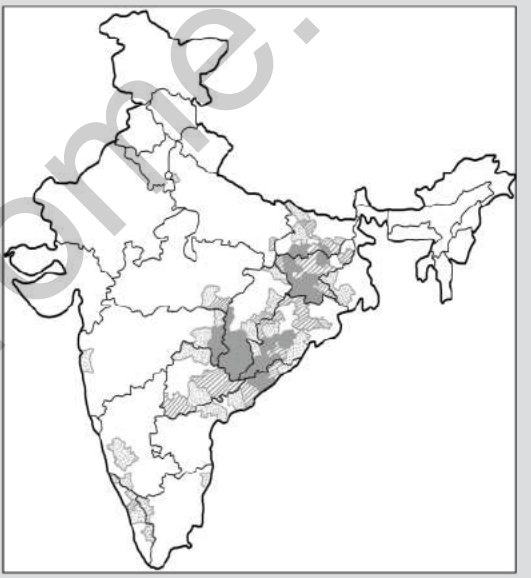
Left Wing Extremism has evolved in **three broad phases** in India: **Phase 1** (1967–1973) – the **formative phase**, **Phase 2** (1967–late 1990s)– the era of **spread of LWE**, and Phase 3 (2004–Current) – relative **decline after brief fightback**. The **first phase** of Naxalism started with the incident of Naxalbari (1967) which led to Formation of All India Coordination Committee of Communist Revolutionaries (AICCCR). They adopted two doctrines: (a) Allegiance to militant struggle and (b) Non-participation in elections. In May 1969, the AICCCR formed a new party, **the Communist Party of India (Marxist–Leninist)**, in short known as CPI(ML).They elected Charu Majumdar as its general secretary. They indulged in armed violence in West Bengal, Andhra Pradesh, Kerala, Bihar, Odisha, Madhya Pradesh, Punjab and Uttar Pradesh. In July 1971, Indira Gandhi government took advantage of President's rule to mobilize the Indian Army against the Naxalites and launched a colossal combined army and police counter-insurgency operation, termed "Operation Steeplechase" killing hundreds of Naxalites and imprisoning more than 20,000 suspects and cadres, including senior leaders. By 1973 the main cadres of the Naxalites had been eliminated and were dead or behind bars. The movement fractured into more than 40 separate small groups.

During the **Second Stage** (1975-2004), Naxals continued their struggle under the 'Strategy of Protracted War'. CPI (ML) got converted into People's war group in 1980. The Peoples' War Group emerged as the dominant group with its active presence not only in Andhra Pradesh but also in Orissa, Madhya Pradesh, Chhattisgarh and Maharashtra. At the same time Moist Communist Centre of India (MCCI) strengthened in Bihar.

During the 1990s, the Naxalist activities got dull due to strict police action but in 2004 Communist Party of India (Marxist–Leninist) People's War (People's War Group) combined with the Maoist Communist Centre of India and formed CPI (Maoist) marking the beginning of the **third stage** of Naxalism. This brought about a renewed spurt of violence. CPI (Maoist) was listed as Terrorist Organisation under the Unlawful Activities (Prevention) Act in 2009. In September 2009, an all-out offensive **(Operation Green Hunt)** was launched by the Government of India's paramilitary forces and the state's police forces against the CPI (Maoist). Since the start of the operation, thousands of Maoist militants have been killed, many more either arrested or surrendered.

Red corridor: It is a region demarcated by the Union Government to notify the areas and districts which are affected by left wing extremism or Naxalism. As of 2021, it spans across 70 total districts in 10 States, out of which 25 are 'most/worst affected' districts accounting for 85% of LWE violence. States affected by LWE include Bihar, Jharkhand, Chhattisgarh, Andhra Pradesh, Maharashtra, Odisha, Telangana, West Bengal, Madhya Pradesh, and Kerala.Sometimes the extent of Naxalism is also referred to as having influence from 'Pashupati (Nepal) to Tirupati (Andhra Pradesh)'. In 2009, 180 districts were included in the red corridor. It has been steadily diminishing in terms of geographical coverage and number of violent incidences. (Based on MHA data)





	2008	2016
Highly Affected	58	25
Moderately Affected	54	31
Marginally Affected	83	48
	District - 195, States - 16	District - 104, States - 13

Maps are based on data from South Asia Terrirosm Portal (SATP), Institute for Conflict Mangement

2.4. CAUSES BEHIND SPREAD OF LWE: LINKAGE BETWEEN DEVELOPMENT AND SPREAD OF EXTREMISM

Any social and political movement, in general, is initiated with an objective based on an issue which is deeply connected to the conditions of life of the people, their dignity and ethos. The movement consists of reactions to the frustrations suffered at the hands of oppressor or unjust authority. The left-wing extremism is also based on numerous causes related to factors such as land ownership, denial of forest rights, livelihood issues, poor governance, etc.

The most important cause of the Left-wing Extremism is the issues surrounding **ownership of land and forest rights**, most commonly called issues of **Jal-Jangal-Jameen**. After independence reforms were initiated in land policy and land ownership, but these were not implemented well in the remote tribal regions where incidences of evasion of land ceiling laws was more common than its adherence. Certain powerful section of the society specially in the backward regions enjoyed special land tenures (exemptions under ceiling laws), they encroached and occupied government and community lands (water-bodies included). No titles or ownership of the land was provided to landless poor even though the land was cultivated

by them. Laws prohibiting transfer of tribal land to non- tribal were poorly implemented in the Fifth Schedule areas. Traditional land rights were not recognised nor documented.

Case Study of Chikpar Village

There is the case of the residents of a village called Chikpar. The village was first acquired in 1968 for the MiG jet fighter project for Hindustan Aeronautics Limited (HAL). The 500 families were evicted, and they were moved to another location (leaving the land they owned) and resettled there. The villagers nostalgically named the new village as Chikpar. In 1987, the families were evicted again for the Kolab multi- purpose project. The villagers were again resettled at another place. However, they received eviction notices for the third time for another development project. Needless to say, the displaced persons were paid a pittance as compensation that too after several years. In 1993, again, they were evicted from Chikpar-3 so that Military Engineering Service could be established there. Thus, it was witnessed that each time the land belonged to the village community but the state just took it and paid less or no compensation.

Another major reason behind the extremism is the **displacement and forced evictions** of villagers, tribal and forest communities in the name of developmental projects. Tribals and other forest communities living in remote but resource rich regions (like river basins, resources like coal, iron) of states Jharkhand, Chhattisgarh, Odisha were displaced for developmental projects like- canals, power projects, dams and mines without adequate rehabilitation measures. It was widely accepted that displacement of tribals or indigenous people was an **'acceptable cost'** based on the narrow and standard interpretation of word 'development' which benefitted only certain sections of society and not all. Tribals and forest dwellers were evicted from the lands traditionally used by them, their sources of livelihood got disrupted and their relationship with forest changed. Though they were evicted /displaced in name of growth and development, fruits of that growth never reached them. The trickle-down theory of growth and capitalist development could not help them achieve a decent standard of living in sync with their natural environment.

Tragic Case of Displacement in the Name of Development

In 1940s, the tribals living in the Chitrakonda in Malkangiri district in Odisha were first displaced from Koraput by Machhkund Hydel Project. The displaced tribals moved to Chitrakonda. But again, in 1960s the already displaced tribal population were again displaced by the Balimela Hydel Project. Since then, their villages remained water locked by the Chitrakonda reservoir and are accessible only by boat. No rehabilitation and socio-economic development took place there for decades. It was only in 2018 that Gurupriya Bridge connecting water-locked island to the mainland was inaugurated.

The **livelihood related issues** faced by the villagers and tribal has also been one of the factors for spread of extremism. The traditional dependence on their natural local and common resources got disrupted due to various government initiatives taken in the name of regional development. Along with this, there was issue of lack of alternative livelihood opportunities. The poor implementation of Forests Rights Act and the reluctance of some forest officials and forest bureaucracy to work towards addressing the issues of the tribal alienated them further. Corruption is also rampant as the lower tier officials and bureaucracy is hands in glove with the private entities/contractors. The tribal have also suffered from food insecurity due to corruption and mismanagement in the Public Distribution System. Their local staple foods were never considered in the PDS system and they were expected to consume rice and wheat instead of millets or other indigenous local grains.

Geoghraphical exclusion and tribal alienation have also been one of the reasons which make tribal and rural communities vulnerable to extremist ideology. The regions affected by Naxalism are remote underdeveloped regions having dense forests, inaccessible terrain, low density of roads and railways leading to geoghraphical exclusion. Combined with this, tribal communities are socially disadvantaged and discriminated sections of society. Their different and unique culture

makes them face prejudices and non-inclusion into mainstream society. Poor implementation of special laws like prevention of atrocities, protection of civil rights and abolition of bonded labour have also alienated them further. In certain states like Bihar, Uttar Pradesh the reasons are not based on issues of tribal or forest communities but points towards centuries of caste discrimination and oppression by higher caste landlords.

Along with the above discussed reasons, **governance related factors** are also a major concern. In such remote underdeveloped regions, corruption in bureaucracy is common. The government administrative officials are apathetic, poorly trained and lack motivation resulting in frequent absence from their office or place of posting. Hence, the people lose faith as the front face of administrative machinery behaves non-concerned and non-empathetic. The governance and delivery of public service in these areas are also in shambles with poor or non-provision of essential public services including electricity supply, primary health care and education. The Constitution of India, under Schedule 5, provides for special arrangement for administration and enhanced autonomy for tribal areas. Through Panchayats (Extension to Scheduled Areas) Act, 1996, the Panchayati Raj system has been extended to the 5th schedule areas for promotion of grassroot democracy. But, non-implementation of provisions of the 5th schedule and PESA has also contributed to the rise of LWE in tribal areas. The institutions of local self-government are inefficient and cannot address the demands of the people. There is absence of grievance redressals systems too. Sometimes police and security agencies misuse their power to subjugate tribal and villagers, that further alienates the people from government. These tribals continue to be neglected and exploited subjects rather than equal citizen of the country.

Schedule 5 and PESA Act, 1996

Fifth schedule includes areas **inhabited by 'aboriginals'** who are socially and economically **backward** and special efforts are needed to improve their condition. Most of the area included in the fifth schedule is also infested with the Left-Wing Extremism. This anomaly exists because of poor/non-implementation of the provisions in the fifth schedule. Special provision exists in the fifth schedule to ensure that the local/tribal people do not get marginalised/alienated. The governor has a special responsibility regarding such areas. The governor has to submit a report to the President regarding the administration of such areas, annually or whenever so required by the President. Further, the executive power of the centre extends to giving directions to the states regarding administration of such areas. Further, each state having scheduled area has to establish a **tribes advisory council** to advice on welfare and advancement of the scheduled tribes. This council is to have 20 members, three fourth of whom are to be the representatives of the scheduled tribes in the state legislative assembly. Also, the Governor is empowered to direct that any particular act of the Parliament or the state legislature does not apply to scheduled area or apply with specified modification and exceptions. The **Governor can also make regulations** for the peace and good government of scheduled area after consulting the tribes advisory council. Such regulations **may prohibit** or **restrict the transfer of land** by or among members of the scheduled tribe, regulate the allotment of land to members of the scheduled tribes and also **regulate the business of money-lending** in relation to scheduled tribe. Also, a regulation may repeal or amend any act of Parliament or the state legislature, which is applicable to the scheduled area, after the assent of the president.

The provision of Part IX of the constitution relating to the Panchayats are not applicable to the fifth schedule areas. However, the Parliament may extend these provisions to such areas, subject to such exceptions and modifications as it may specify. Under this provision, the Parliament has enacted the **"Provisions of the Panchayats (Extension to the Scheduled Areas) Act", 1996,** popularly known as the PESA Act. In accordance with this act a state legislation on the Panchayats in scheduled areas shall be in consonance with customary law, social and religious practices and traditional management practices of community resources. Further, every village shall have a Gram Sabha consisting of persons whose names are included in the electoral rolls for the Panchayat at the village level.

Gram Sabha shall **approve the plans, programmes and projects** for social and economic development before they are taken up for implementation by the Panchayat at the village level. Also, the Gram Sabha or the Panchayats at the appropriate level shall be **consulted** before making the **acquisition of land** in the scheduled areas for the projects. In addition, planning and **management of minor water bodies** in the Scheduled Areas shall be entrusted to Panchayats at the appropriate level. Moreover, the state legislature should ensure that Panchayats and Gram Sabhas are endowed specifically with: a) the power to **enforce prohibition** or to regulate or restrict the sale and consumption of any intoxicant, b) the **ownership of minor forest produce,** c) the power to **prevent alienation of land** in scheduled areas, d) the power to exercise control over money-lending to scheduled tribes, e) the power to exercise control over institutions and functionaries in all social sectors. Also, the state legislature should ensure that Panchayats at higher level do not subsume the powers and authorities of Gram Sabha.

These exhaustive provisions were meant to mainstream tribal people, reinforce their control over natural resources, prevent their exploitation/alienation, promote decentralized governance and to preserve their local culture. However, non-**implementation of these provisions** has caused loss of control of local people over natural resources. There exploitation at the hands of big corporates has become an on-going curse. The **loss of local culture, traditions and values** have caused irreparable **damage to the tribal identity**. Lack of good governance and decentralization of power have prevented the dividends of growth from reaching the last mile. This has given a ready **fodder for the violent anti-state leftist ideology** to flourish.

Q. Article 244 of the Indian Constitution relates to administration of schedules area and tribal areas. Ana-lyse the impact of non-implementation of the provisions of the Fifth schedule on the growth of Left-Wing extremism. **(UPSC 2013)**

These reasons were corroborated by the expert committee under D Bandopadhyay constituted by the Planning Commission in 2006 which also said that there are two main reasons for spread of Naxalism, which viz. lack of empowerment of local communities and failure of state bureaucracy to deliver good governance.

2.4.1. Urban Naxalism

Until recently, Naxalism was associated with left-wing extremist groups that operate in treacherous terrains of jungles and backward rural areas, with leadership being provided by educated people initially residing in urban areas (like Charu Mazumdar), while the tribal and villagers acted as mere foot soldiers. But in recent years, there have been instances of educated, employed people belonging to urban areas propagating Maoist agenda. They could be teachers, professors, activists, celebrities and influencers influencing the urban intelligentsia to their cause. This phenomenon has been called as Urban Naxalism.

Bollywood movie, Buddha in a Traffic Jam is based on the theme of urban naxalism. Its shows how young people are exposed to LWE literature and slowly brainwashed into LWE activities.

Few recent incidents have highlighted the debate on urban Naxalism. Though there have been allegations of non-state activities and spreading of Maoist far left ideology by certain people in urban areas, the debate has been raging if the present term 'urban naxals' is just a new term for anti-nationals or dissenters of government policies. A major group of the Kerala Naxal cadre was busted in 2015. It was found that the group was led by a well-educated engineer who had written novels on themes of Naxalism and they were planning to enter Chennai to establish their network. They had support of many intellectuals too. In March 2017, a professor of Delhi University was convicted under charges of spreading Maoist propaganda. It was said that the professor had been working closely with Naxals to create propaganda material for circulation among urban centres. The Maharashtra police arrested five prominent activists in connection with an ongoing

investigation related to the Bhima-Koregaon caste flare up in January 2018. In addition, the police had presented a sensational letter implicating all five accused in hatching a plot to assassinate the Prime Minister of India. The police conducted raids and arrested these well-known activists naming them as "urban Naxals". This case took a turn when the NIA took charge on the case of Elgar Parishad. Many prominent activists and lawyers were arrested in relation to this, many of them still languishing in jails (till December 2021).

However, Urban Naxalism is an old Maoists strategy to focus on urban centres for leadership, organise mass support, build a united front and engage in military tasks such as providing personnel, material and infrastructure. Urban naxalism is a direct consequence of two documents which were released after formation of CPI(Maoist) (formed after merger of splinter groups in 2004): 'The Strategies and Tactics of Indian Revolution in 2004' and 'Urban perspective: Our work in urban areas'. A systematic approach was initiated by the CPI-M to mobilise resources and achieve the objectives through urban mobilisation, taking advantage of the anonymity in the urban centres. 'Urban perspective: Our work in urban areas' stated new strategy to be employed focussing on a six-stage approach called SAARRC – survey, awareness, agitation, recruitment, resistance and control.

However, their urban surge has proved a disaster for Naxals as they lost many of their top leaders. Their ideologues like Narayan Sanyal, Amitabh Bagchi, Kobad Ghandy were arrested by security forces from their urban hidings.

2.5. ISSUES IN HANDLING LWE

LWE has been a pertinent threat for over 60 years, however, intensity and frequency of violence have varied. Eliminating the threat of left-wing extremism is not an easy task, as there are numerous issues in handling the problem. Some of them have been discussed in this section.

As Police is a state subject, **lack of inter-state police coordination** leads to Naxalites using other state as new locations of operation. When paramilitary and police forces push Naxals out of a region, they use other states to regroup and rearm. This can be associated with the case of use of special forces like Greyhounds by AP and Telangana which led to spill over to other states. The trijunction of Maharashtra, Chhattisgarh and Telangana having dense forests and difficult terrain acts as refuge for the Naxalites.

Naxals are also known to **collaborate with other insurgent groups** who are essentially ideologically different but are anti-state. According to intelligence report in 2008, Left-wing extremists approached militant groups like ULFA in Assam and LTTE in Sri Lanka for procurement of arms and explosives. Collaboration with international Maoist movements and funds by foreign anti-state actors are other major issues in tackling the Naxalism problem. Naxal leaders operating in Bihar and Jharkhand are known to launder extorted money by acquiring movable and immovable assets.

On administrative side, lack of proper **infrastructure**, poor **connectivity** (mobile and roads) and shortage of trained **manpower** are some of the issues faced in governance. Extremists destroy infrastructure like schools, hospitals which leads to increase in social and physical infrastructure deficit in the region. In some parts of Dandakaranya region in Chhattisgarh, Maoist ran parallel governments called 'Janatana Sarkar', which made administration by the government agencies difficult. Poor coordination among various state police forces also lead to inadequate planning. Negligence of established standard operating procedures at times leads to loss of valuable lives of security personnel. The capacity building of police forces is quite sluggish, a fact corroborated by thousands of vacancies in different ranks in state police force and many sanctioned police stations yet to be set up. Inefficient technology of underground mine detection has led to loss of precious civilian and personnel lives. There has been delay in acquisition of technology like out of all the sanctioned Multi-Purpose Vehicles, only few in number have been supplied by Ordnance Factory Board to CAPFs.

2.6. MEASURES TAKEN BY GOVERNMENT TO SOLVE THE ISSUE OF LWE

The Government of India takes a multipronged approach based on carrot and stick policy to deal with left wing extremism (LWE) focussing on areas like security, development, ensuring rights and

entitlements of local communities, improvement in governance and public perception. After various high-level deliberations and interactions with the state governments concerned, it has been agreed that an integrated approach, focussing on better developmental indicators and strict crackdown on naxal cadres would deliver results. **LWE Division** was created in 2006 in the Ministry of Home Affairs, to effectively address the Left-Wing Extremist insurgency. Its tasks are to implement security related schemes aimed at capacity building in the LWE affected States, to monitor the LWE situation and counter-measures being taken by the affected States. The LWE Division coordinates the implementation of various development schemes of the Ministries of Government of India in LWE affected States.

In pursuit of the above stated approach, Ministry of Home Affairs has been implementing **'The National Policy and Action Plan'** since 2015 as a multi-pronged strategy dealing in areas like security, development, ensuring rights & entitlement of local communities to combat Left Wing Extremism (LWE). In 2017, SAMADHAN strategy was launched by MHA to frame short term and long-term policies to tackle LWE. It includes:

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

Operation Ghamasan

Operation Ghamasan meaning 'fierce', is the Maoist's attempt to counter, Operation SAMADHAN - the strategy launched by the government to exterminate Naxalite insurgency. Operation Ghamasan purportedly intends to build an 'anti-fascist front' and calls upon broad mass participation including youth, intellectuals and women to join in its cause. It revolves around the **triumvirate** of armed struggle, mass mobilization and opening new fronts of struggle along with self-rectification.

'Police' and 'Public Order' are State subjects as per the seventh Schedule of the Constitution. However, the efforts of the States for equipping and modernizing of their police forces has been supplemented by the Government of India through the scheme of "**Assistance to States for Modernization of Police (ASMP)**" [erstwhile scheme of Modernization of Police Forces(MPF)]. Under the scheme, the State Governments are provided central assistance for acquisition of latest weaponry, training gadgets, advanced communication / forensic equipment, cyber policing equipment etc. Further, 'construction' and 'purchase of operational vehicles' are permitted in the insurgency affected north-eastern States and Left Wing Extremism (LWE) affected districts. As such, under the scheme financial assistance is provided for acquisition of infrastructure and equipment, including training equipment, which enhances capabilities and efficiency of the police forces.

As a part of **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. Road Connectivity Project for LWE affected areas (RRP-II) was approved in 2016 for further improving road connectivity in 44 districts of 9 LWE affected States. **LWE Mobile Tower Project** has been initiated to improve mobile connectivity in the LWE areas. Projects have been approved under Universal Service Obligation Fund (USOF) to provide mobile services in 96 districts of LWE-affected states.

For improving the operational performance of the CAPFs in the LWE affected region, the MHA approved the use of cutting-edge **technology** by the paramilitary forces like trackers for weapons, bio-metrics for smart guns and a Unique Identification Number (UID) for gelatine sticks and explosives. The National Technical Research Organization (**NTRO**) is assisting the Security Forces in anti-Naxal operations by providing Unmanned Aerial Vehicles (UAVs). **Black panther combat force**, based on Greyhounds of AP and Telangana, has been raised for operation in Chhattisgarh. **Bastariya Battalion** of CRPF with tribal youth having adequate female representation from four highly Naxal infested districts of Chhattisgarh has

been setup, making it the first composite battalion in any of paramilitary forces. A process has also been initiated to create a **separate vertical in the NIA** for investigating important cases relating to Left Wing Extremism (LWE). MHA has also formed **multi- disciplinary groups** with officers from central agencies, including from the IB, NIA, CBI, ED and DRI, and state police to choke the **financial flow** to Maoists.

Salwa Judum: It began in 2005 as a government-backed 'people's resistance movement' against the Maoists. In the Gondi tribal language, Salwa Judum means 'peace march'. It involved authorities arming tribal villagers to fight the Maoists. The militia, consisting of local tribal youth, received support and training from the Chhattisgarh state government. There were reports of human rights violations by the Judum. In 2011, the Supreme Court delivered a historic judgment in **Nandini Sundar and others vs the State of Chhattisgarh case.** The judgment aimed to curb the misuse of power by the government and protect tribal rights. It declared the militia to be illegal and unconstitutional and ordered its disbanding. The Court directed the Chhattisgarh government to recover all the firearms, ammunition and accessories and criticized it for its violations of human rights and recruiting poorly trained youth for counter-insurgency roles.

National Technical Research Organisation: The NTRO is a dedicated technical intelligence agency created after the 1999 Kargil war. It has listed as an intelligence organization under The Intelligence Organisations (Restriction of Rights) Act, 1985.

Along with several infrastructural schemes, the Government of India is also executing several schemes under the **Pradhan Mantri Kaushal Vikas Yojana (PMKVY)** that are empowering the citizens with the required skill sets to earn their livelihood. Under this programme 47 Industrial Training Institutes (ITIs) and 68 Skill Development Centres (SDCs) were targeted to be established by March 2019. **ROSHNI** is a special initiative under Pandit Deen Dayal Upadhyaya Grameen Kaushal Yojana which envisages training and placement of rural poor youth from 27 LWE affected districts. ITIs and Skill Development Centres have been established since 2011-12 in LWE affected districts. Many LWE affected districts are part of **Aspirational District Programme (ADP)** of NITI Aayog. ADP is based on 49 indicators from the 5 areas, which focuses on improving people's Health & Nutrition, Education, Agriculture & Water Resources, Financial Inclusion & Skill Development and Basic Infrastructure.

In an attempt to reassimilate Maoists into mainstream society suitable **surrender and rehabilitation policies** have been formed. 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. For constructively engaging youth through education, **Eklavya schools**, use of Porta cabins as classrooms , an educational hub and a livelihood centre in Dantewada district has been initiated. The Chhattisgarh government has opened livelihood centres known as **Livelihood Colleges** in 27 districts. More bank branches have been opened in tribal and rural areas to ensure **financial inclusion**. All India Radio stations in the three southern districts of Bastar now broadcast regional programmes to increase entertainment options. A proposed rail service in Bastar is expected to throw open a new market for wooden artefacts and bell metal.

Eklavya Model Residential Schools (EMRSs) is a flagship intervention of the Ministry of Tribal Affairs, Government of India to provide quality **residential education** to Scheduled Tribes students from Class 6th to 12th in remote areas to enable them to access the best opportunities in education and to bring them at par with the general population. The programme has been in operation since 1998 and was revamped during the year 2018-19 to expand the geographical outreach and enhance the quality of facilities.

2.6.1. Some Success Stories

1. **Andhra Pradesh model**: Andhra Pradesh's Greyhound fighting force along with developmental projects and implementation of surrender and rehabilitation policy has proved effective. The successful elements

in the Andhra Pradesh model are sound knowledge of local terrain, incentives being provided to police for good work, operations undertaken based on local intelligence and most importantly grass roots involvement in anti-Naxal operations .

2. **Sandesh (Bihar)**: Sandesh block in Bihar has seen a gradual elimination of Naxalites. The most important factor which proved instrumental in dismantling Naxal dominance was the initiation of grassroots democracy in the form of panchayat elections. It created a significant distance between the Naxal leaders and the local community. Social pressure forced many Naxalites to switch over to farming and terminate their association with Naxal outfits.
3. Under the **Integrated Action Plan (IAP)** under which the centre directly released Rs 1,500 crore to LWE affected districts and left it to the discretion of a district-level committee comprising the collector, SP and district forest officer to earmark the development and infrastructure projects. The district administration spent the amount on works ranging from setting up of drinking water facilities and sanitation to construction of school buildings, roads and health centres and electrical lighting. The erstwhile Planning Commission said, "IAP is a success wherever the district administration has taken keen interest in development activity".

2.7. RECENT DEVELOPMENTS

The problem of LWE or Naxalism continues to rank high in the list of internal security challenges that the country faces but past few years have seen an improvement in the LWE scenario. As per the **2019-20 annual report of Ministry of Home affairs**, there has seen a **significant decline in LWE violence** as well as the geographical spread of LWE. There has been an overall 41% reduction in violent incidents (1136 to 670) and 49% reduction in LWE related deaths (397 to 202) in 2019 as compared to 2013. In comparison to 2018 also, the year 2019 saw a decline of 19% (833 to 670) in incidents of violence and 15% in the number of resultant deaths (240 to 202). The casualties to Security Forces declined by 22% (67 to 52) and the number of LWE cadres eliminated also declined by 35% (225 to 145). At the same time, the developmental outreach by the Government of India has seen a large number of LWE cadres shunning the path of violence and returning to the mainstream.

Success in control of LWE is also corroborated by **shrinkage of geographical area** affected by LWE. MHA in 2018, redrew the Red Corridor by bringing down the number of districts affected with Naxal violence from 106 to 90, spread across 11 states and worst-affected district to 30 from 36. Chhattisgarh, Jharkhand, Odisha and Bihar were declared severely affected by LWE. Total of 44 districts were removed from the list and eight new districts which could be slightly or partially affected were added to the list. In 2021, areas affected by LWE has further shrunk to just 70 districts, out of which only 25 are categorized as 'worst affected'.

The overall improvement in the LWE scenario can be attributed to greater presence and **increased capacity of the Security Forces** across the LWE affected States, better **operational strategy** and better monitoring of **development schemes** in affected areas. Greater presence of security forces across the LWE affected States and creation of special forces like Greyhound, Bastariya battalion have led to less violent incidents. There has been a continuous loss of cadres/leaders on account of arrests, surrender and desertions. A comprehensive offensive strategy of **SAMADHAN** with focus on **intelligence, financing, technology, training etc.** has been deployed to confront LWE There has also been an insurgency fatigue among the Maoist cadres after so many years of fight and violence. There has been a shortage of funds, arms and ammunitions too due to curbs on terror financing.

The Rehabilitation program of government has been a success where many have surrendered and taken up a normal violence free life. Good governance has led to better monitoring of developmental schemes in affected areas. States have been working effectively to implement the provisions of **PESA, 1996** and **Forest Rights Act 2006**. Security forces have undertaken various welfare activities under the **Civic Action Program.** To counter the **ideological arguments of LWE** about exploitation by state, initiatives like **Tribal Youth Exchange programs** try to reduce trust gaps.

Mines and Minerals Act was amended to setup **District Mineral Foundation** for development of tribal areas, ensuring local ownership of resources. Some experts claim that **Covid-19 pandemic** also impacted LWE activities as their movement was restricted and mobilizing people during lockdowns was difficult. The pandemic also created fear of an unknown disease which spreads quickly resulting in confusion, splintering of large groups and inability to execute violent incidents.

However, the left wing extremists are targeting new States and are trying to carve out the base at the tri-junction of Karnataka, Kerala and Tamil Nadu.

2.8. TOWARDS A BETTER FUTURE

The **root cause** of the problem should be **eliminated** through development focussed on the vulnerable sections. The enhanced emphasis should now be on building rural roads, increasing administrative and political access of the tribals, improving reach of government schemes and eliminating corruption in administration etc. **The Scheduled Tribes and other Traditional Forest Dwellers (Recognition of Rights) Act, 2006** should be effectively implemented in letter and spirit to address livelihood and forest rights of tribals. Formation of 'Self Help Groups' (SHGs) to improve access to credit and marketing and empower the people should be encouraged to help financial inclusion.

Implementation of large **infrastructure projects**, like road networks need to be undertaken with the help of **specialised Government agencies** like the Border Roads Organisation instead of local contractors. Special efforts are needed to monitor the implementation of constitutional safeguards, development schemes and land reforms initiatives for eliminating discontent among sections vulnerable to the propaganda of violent left extremism. Along with this, government should undertake **awareness and outreach programmes** for good governance.

Centre and states should continue with their coordinated efforts where Centre should play a supportive role with state police forces taking the lead. In this, lessons can be learnt from Chhattisgarh police. As the Chhattisgarh police have experience in tackling Maoists in Bastar, they are now coordinating with the bordering States to strengthen intelligence and ground presence. Also, steps should be taken to choke sources of funds for the extremist activities with the help of intelligence agencies and international cooperation.

To **bridge the trust deficit**, civil society must join hands with the government in implementing the villagers' right to development. The nexus between illegal miners/forest contractors providing financial support to extremists needs to be broken through establishment of special anti-extortion and anti-money laundering cell by State Police. Undertaking technological solutions, such as use of UAVs or small drones to minimize loss of lives of security personnel.

Successful implementation of various development initiatives focusing on critical issues of **Jal (water), Jamin (land) and Jungle (forest)** has been the most important factor in making the LWE movement difficult to sustain itself on a large scale. The two-pronged policy of direct action by the security forces combined with development is showing results. The government has already made a dent in most of the affected districts and is determined to check the expansion and curtailing of Maoist activities.

Q1. What are the determinants of left-wing extremism in Eastern part of India? What strategy should Government of India, civil administration and security forces adopt to counter the threat in the affected areas? **(UPSC 2020)**

Q2. Left Wing Extremism (LWE) is showing a downward trend, but still affects many parts of the country. Briefly explain the Government of India's approach to counter the challenges posed by LWE. **(UPSC 2018)**

Q3. The persisting drives of the government for development of large industries in backward areas have resulted in isolating the tribal population and the farmers who face multiple displacements. With Malkangiri and Naxalbari foci, discuss the corrective strategies needed to win the Left-Wing Extremism (LWE) doctrine affected citizens back into mainstream of social and economic growth. **(UPSC 2015)**

Terrorism

3.1. INTRODUCTION

Terrorism is a **global crime** and has gained importance at the international and regional level as a subject of concern. The political, economic and diplomatic affairs of the world are influenced by the grave threat of terrorism. India is **surrounded by hostile nations**, which are considered as the **hotbed of terrorist activities**. Problem of porous borders with the same nations pose as huge threat to internal security and law and order.

Terrorism encompasses a range of **complex threats** viz. organized terrorism in conflict zones, foreign terrorist fighters, radicalized 'lone wolves', and attacks using chemical, biological, radiological, nuclear and explosive materials. Terrorist groups incite individuals, often young people, to leave their communities across the world and travel to conflict zones, such as in Iraq, Syria, Libya etc. The way recruits are targeted and radicalized has shifted, with greater focus on social media and the digital channels. The term "terrorist" originated during the French Revolution of the late 18th century but became widely used internationally during the 1970s, when events like **Northern Ireland conflict, the Basque conflict, and the Israeli-Palestinian conflict** gained worldwide attention. September 11 attacks in the United States, introduced the world with the spectre of suicide attacks. Lone wolf attacks/fidayeen attacks etc., have now become common modus operandi for the terrorist organizations across the world.

3.1.1. Historical Background

Terrorism is as old as the Roman Empire and it existed in the form of Zealots in Judea or the Assassins in the 11th to 13th century with religion being a strong motivating factor behind terrorist activities. The term "terrorism" originated from the Reign of Terror (Regime de la Terreur) of 1793-94. Some of the freedom fighters of Indian Independence struggle like Khudiram Bose, Prafulla Chaki , Chapekar brothers were termed as revolutionary terrorists by the colonial government. The Second World War, however brought a shift in the nature and locale of terrorist activities around the world. The focus of terrorist activities shifted from **Europe to the Middle East, Africa and Asia** with the various active nationalistic and anti-colonial groups in the regions of Israel, Kenya, Cyprus, Algeria, Palestine and Malaya. International terrorism today is marked by the large number of transnational terrorist groups, mostly motivated by the Islamist fundamentalist ideology like ISIS, Boko Haram, Al-Shabab etc.

The Cold war legacy and the disintegration of states post-Cold War, in a world awash with advanced conventional weapons and know-how, has assisted the proliferation of terrorism worldwide. Instability created by absence of governance in areas such as Balkans, Afghanistan, Columbia, and certain African

countries offered opportunities to fundamentalists and ready-made areas for terrorist training and recruitment activity. Afghanistan, since the 1989 Soviet withdrawal, emerged as a terrorist training ground. Pakistan which has a policy to use terrorism as a foreign policy tool, provides assistance to terrorist groups both in Afghanistan and Kashmir while acting as a further transit area between the Middle East and South Asia. State sponsored terrorism by Pakistan ensures logistical support, easy travel documentation and training facilities for these terrorist organizations. Since 1989 the increasing willingness of religious extremists to strike targets outside immediate country or regional areas underscores the global nature of contemporary terrorism. The 1993 attack on the World Trade Centre, September 11, 2001, attacks on the World Trade Centre and Pentagon, are representative of this trend.

3.2. DEFINING TERRORISM

The report on the **Global Terrorism Index 2020** says that "Defining terrorism is not a straightforward matter. There is no single internationally accepted definition of what constitutes terrorism, and the terrorism literature abounds with competing definitions and typologies." This is because the meaning and interpretation of terrorism changes from region to region and with passage of time. The most apt example for this is of Taliban, which was termed a terrorist organisation after the 9/11 attacks but situation changed in August 2021 when it formed government in Afghanistan. There have been some proposals to outline the definition of terrorism.

The definition of terrorism as proposed by the Secretary General of the UN in September 2005, is that "any act meant to injure or kill the civilians and the non-combatants, in order to intimidate a population, a government, or an organization and incite them to commit an act against the perpetrators or on the contrary stop them from doing so". The **Unlawful Activities Prevention Act, 1967** (amended in 2008)- India's 'anti- terror law' defines a **terrorist act** as "Whoever does any act with intent to threaten or likely to threaten the unity, integrity, security, economic security or sovereignty of India or with intent to strike terror or likely to strike terror in the people or any section of the people in India or in any foreign country".

The definition of terrorism as proposed by the Secretary General of the UN in September 2005, is that "any act meant to injure or kill the civilians and the non-combatants, in order to intimidate a population, a government, or an organization and incite them to commit an act against the perpetrators or on the contrary stop them from doing so". The **Unlawful Activities Prevention Act, 1967** (amended in 2008)- India's 'anti- terror law' defines a **terrorist act** as "Whoever does any act with intent to threaten or likely to threaten the unity, integrity, security, economic security or sovereignty of India or with intent to strike terror or likely to strike terror in the people or any section of the people in India or in any foreign country".

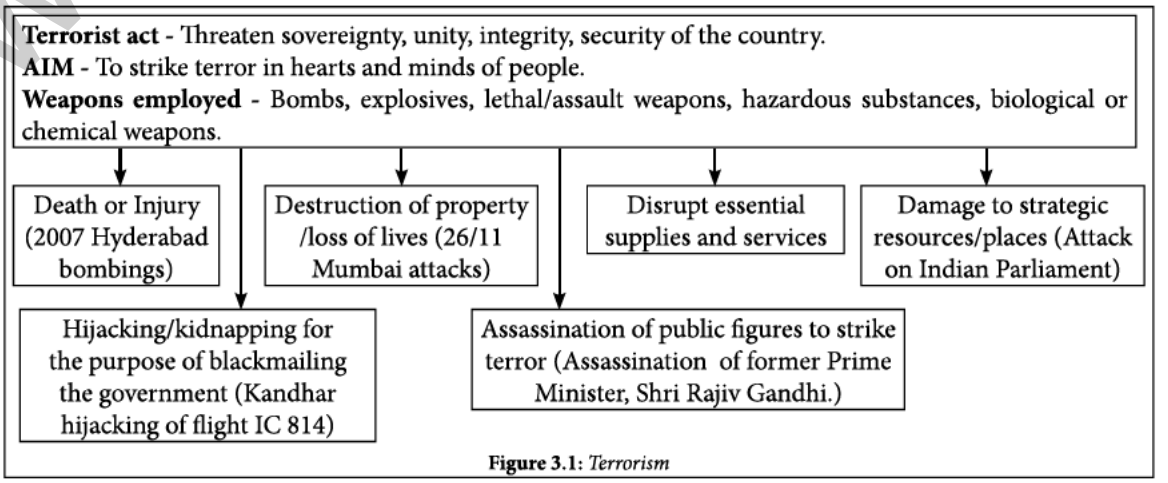


Figure 3.1: *Terrorism*

Some of the **defining characteristics of Terrorism** are the threat or use of violence to achieve immediate objectives, a political objective or ideology supporting the terrorism with the desire to change the status quo. The terrorists have an intention to spread fear by committing public acts of violent nature targeting civilians or public infrastructure. The terrorist act is usually committed by foreign nationals with or without the support of local residents.

3.2.1. Difference Between Terrorism, Insurgency and Extremism

A country like India is battling all types of internal security threats namely terrorism, insurgency, extremism. Though these all acts are aimed against the state, there are subtle differences between terrorism, insurgency and extremism. **Terrorism** is the planned, **organised and systematic** use of violence as a means of coercion for political, religious and ideological purposes. Few examples of banned terrorist organisations of India are SIMI

(Student Islamic Movement of India), LeT(Lashkar e Taiba) etc. Insurgency on the other hand is the act of **rebellion and armed struggle by a section of population** harbouring grievances and with the goal of overthrowing the **lawfully established government**. The insurgents are the nationals of the same country and enjoy local population support. They generally target security forces and state apparatus. The insurgency in North East India is a prominent example. **Extremism** is defined as the holding of extreme religious or political views. **Naxalism or Left Wing Extremism** is the most prominent example of extremist activities in India. It is carried out with the purpose of establishing a **new order of society by violence and to destabilise the state through communist guerrilla warfare activities**. Naxalism in India is based on Maoist ideologies through which they want to overthrow the government by people's war and to install people's government at the helm. Insurgency and Naxalism are different forms of terrorism but all terrorism is not insurgency or Naxalism. (covered in detail in Left Wing Extremism Chapter)

3.2.2. Types of Terrorism

Eighth Report of the Second Administrative Reforms Commission (ARC) which deals with the menace of **terrorism** says that terrorists are motivated by different goals and objectives and depending on these objectives, the nature of terrorism also differs. Globally, the commonly identified major types of terrorist operations include **Ethno- nationalist terrorism, religious terrorism, ideology oriented terrorism , state-sponsored terrorism and narco terrorism.**

Ethnic or ethno-nationalist terrorism is defined as a deliberate violence by a sub-national ethnic group to advance its cause. Ethno-nationalism is defined as the desire of a group of persons having a separate unique ethnic identity to disassociate themselves from the existing government and form a new nation with the help of terrorist organisations and terror activities. Such violence usually focuses either on the creation of a separate State or on the elevation of the status of one ethnic group over the others. Insurgent groups in North East India and Tamil Nationalist groups in Sri Lanka (LTTE) are examples of ethno-nationalist terrorist activities. The other examples are Hamas with the objective of creating a separate state, Palestine and Chechen terrorist organisations of Russia.

Liberation Tigers of Tamil Eelam: LTTE was a Tamil militant organization based in the north-eastern Sri-Lanka, formed to create an independent state in the Tamil majority areas of the Sri Lanka. LTTE was formed as a reaction to the state policies of successive Sri Lankan governments that were widely considered to be discriminatory towards the ethnic Sri Lankan Tamils. Anti-Tamil pogroms in 1956 and 1958 carried out by majority Sinhalese, had the character of planned ethnic cleansing, which inspired many Tamilians to pick up arms. Later, LTTE itself resorted to forcibly removing/ethnic cleansing of Sinhalese and Muslim inhabitants from areas under its control. LTTE was one of the first terrorist organization that used suicide vests for conducting suicide attacks. Former Indian Prime Minister, Mr. Rajiv Gandhi, was a victim of such a terrorist attack by LTTE militant.

Religious terrorism is the one where terrorists are motivated wholly or partially by religious ideals and consider violence as their 'divine duty' or a 'sacramental act'. Basing themselves on religious texts or staunch conservative religious ideals, they try to legitimise and justify their acts of terror. These factors make religious terrorism unique in brutality and is one of the most feared forms of terrorism. One of the most prominent examples was **ISIS's** agenda of creating Islamic Caliphate.

In **Ideology oriented terrorism,** any ideology can be used to support the use of violence and terrorism. Ideology oriented terrorism is generally classified into two: Left-wing and Right-wing terrorism. The instances of the **exploited poor class getting motivated by leftist ideologies** and resorting to violence against the elite class have occurred time and again in the history of mankind. However, the ideological basis for the leftist oriented violent movements was inspired by the **writings of Marx and Engels**. This was supported by the writings and speeches of later communist leaders like Lenin and **Mao Tse-tung (Mao Zedong)**. Leftist ideologies believe that all the existing social relations and state structures in the capitalist society are exploitative in character and a revolutionary change through violent means is essential. Examples of leftist ideologies that have resorted to the use of terror are numerous. These include, the Red Army Faction or Baader Meinhof Gruppe in the former West Germany, Maoism/ Naxalism in India, FARC of Colombia, People's Revolutionary Army of Argentina.

Terrorist Organizations

Al-Qaeda: Established by Osama Bin Laden in 1990s, it aimed to coordinate a transnational mujahideen network, to 'reestablish a Muslim State' throughout the world. This organization encouraged/ radicalized youth to take up arms against its targets, primarily USA and Israel. Al Qaeda serves as the core of a loose umbrella organization that includes members of many Sunni Islamic Extremist groups, including factions of Egyptian Islamic Jihad (EIJ), the Gama'at al-Islamiyaa (IG), and the Harakat ul-Mujahidin (HUM). Al Qaeda orchestrated the bombings of the US embassies in Nairobi, Kenya and Dar Es Salaam, Tanzania etc. Al Qaeda was responsible for the dastardly Sept. 11 attacks in New York.

Harakat ul-Mujahidin: Formerly a part of the Harakat al-Ansar (HUA), the Pakistani-based HUM operates primarily in Kashmir. HUM is thought to have several thousand-armed supporters located in Pakistan occupied Kashmir, and India's southern Kashmir and Doda regions. In 1989, at the end of Soviet-Afghan war, the group entered Kashmiri politics by use of militants under the leadership of Sajjad Afghani and Muzaffar Ahmad Baba. Apart from India the group is designated as a terrorist organization by United Kingdom, United States of America, Bahrain and Canada.

Lashkar-e-Taiba (LeT): LeT is a terrorist organization based in Pakistan, working against India. It was founded during the Soviet-Afghan war by Hafiz Saeed with funding from Osama Bin Laden. The organization is believed to be supported by the Pakistan's Inter-Services Intelligence (ISI). The organization is designated as a terrorist organization by the United Nations under the UNSC resolution 1267. Though it is formally banned by Pakistan, many western and Indian scholars believe that it continues to get support from Pakistan's ISI. LeT was behind the dastardly 2008 Mumbai attacks.

ISIS: Islamic State of Iraq and Syria aka Islamic State of Iraq and Levant is a terrorist organization that follows the Salafi jihadist doctrine. ISIS was formed by Abu Musab al-Zarqawi. It gained world wide recognition when it defeated the Iraqi security forces and took over the Iraqi city of Mosul. In June 2014, the group proclaimed itself a worldwide caliphate. As a caliphate, it claimed religious, political and military authority over all Muslims worldwide. The United Nations has proclaimed ISIS as a terrorist organization and held it responsible for various human rights abuses, genocides, war crimes, and crimes against humanity. ISIS uses social media sites such as twitter, telegram to disseminate its propaganda through images and videos. Though ISIS has relatively less influence in India, still many youths have fallen prey to its radicalizing tactics.

Jaish-e-Mohammad: Jaish-e-Mohammad is a Pakistan based Deobandi Jihadist terrorist group largely active in Kashmir. The group has the stated objective of separating the Union Territory of Jammu and Kashmir(erstwhile state) from India, and merge it into the state of Pakistan. Jaish-e-Mohammad maintains a close link with the Taliban and Al Qaeda. Experts believe that JeM was created with the support of Pakistan's Inter-Services Intelligence (ISI). JeM was involved in some of the deadliest terrorist attacks on Indian territory. The 2001 Indian Parliament attack, 2016 Pathankot airbase attack, the 2016 Uri attack, 2019 Pulwama attack etc., are all attributed to JeM.

Babbar Khalsa International: Babbar Khalsa International (BKI) is a Sikh terrorist organization whose main objective is to create an independent Sikh country - **'Khalistan'**. It is operational with activities seen across the globe in countries like United States of America, United Kingdom, Canada, Japan, apart from India. BKI was created in 1978 by Talwinder Singh Parmar, it is notorious for killing of 329 civilians in Air India Flight 182 and for 1985 Narita International Airport bombing. The group receives funds and support from its supporters within the Sikh community, that are largely located in Europe and North America. BKI is officially banned and designated as an international terrorist organization by several countries including UK, USA, Canada and India.

FARC of Columbia

The Colombian armed conflict (1964 - 2016) is the oldest armed conflict in the Americas, beginning in 1964 with the creation of the Revolutionary Armed Forces of Colombia (Fuerzas Armadas Revolucionarias de Colombia- FARC), the largest of left-wing guerrillas groups which have operated in the country. Colombia signed a peace deal with the Revolutionary Armed Forces of Colombia (FARC) at the end of 2016, which ended the rebel group's part in five decades of conflict that has left more than 260,000 dead and millions displaced.

Right-wing groups generally seek to **maintain the status quo** or to return to some past situations that they feel should have been conserved. They have reactionary tendencies in them and their jingoist ideology ensures them to resort to violence so that their demands be met. Sometimes, groups espousing rightist ideologies might assume **ethnic/ racist character** too. They may force the government to acquire territory or to intervene to protect the rights of an 'oppressed' minority in a neighbouring country, for example, the Nazi Party in Germany. Violence against migrant communities also comes under this category of terrorist violence. It is to be noted here that religion can play a supportive role in rightist violence. Some of the examples of these are **Nazism in Germany**, the Fascists in Italy, white supremacy movements in the US known as the **Ku Klux Klan (KKK)** etc. The 2008 Malegaon blasts was an act of Hindu Right wing terrorism.

In recent times, some countries have embraced terrorism as a **deliberate instrument of foreign policy**. One distinction of **state-sponsored terrorism** from other forms of terrorist activity is that it is initiated to obtain certain clearly defined foreign policy objectives rather than grabbing media attention. Having this characteristic, it operates under fewer constraints and causes greater casualties on the target nation. For example, Countries like Iran, Iraq, Sudan, Libya North Korea have been engaged in sponsorship of political violence of different nature in their 'enemy' countries. India has been facing this problem from Pakistan for quite a few years in the form of Lashkar-e- Taiba (LeT) which has been sponsored by ISI, the intelligence agency of Pakistan.

Operation Tupac/Topac: Operation Topac is the alleged codename of an **ongoing military-intelligence contingency program** that has been active since the 1980s and run by the **Inter-Services Intelligence of the Pakistan**. It is aimed at providing covert support to anti-India separatists and militants in Jammu and Kashmir. It is believed by the scholars that under this program ISI helped create six separatist militant groups in Jammu and Kashmir, including Lashkar-e-Taiba.

Another type of terrorism is **Narco-terrorism** which is the attempt by 'narcotics traffickers' to influence the policies of the Government by **systematic threat or by violence**. As the term itself suggests, narco-terrorism combines two criminal

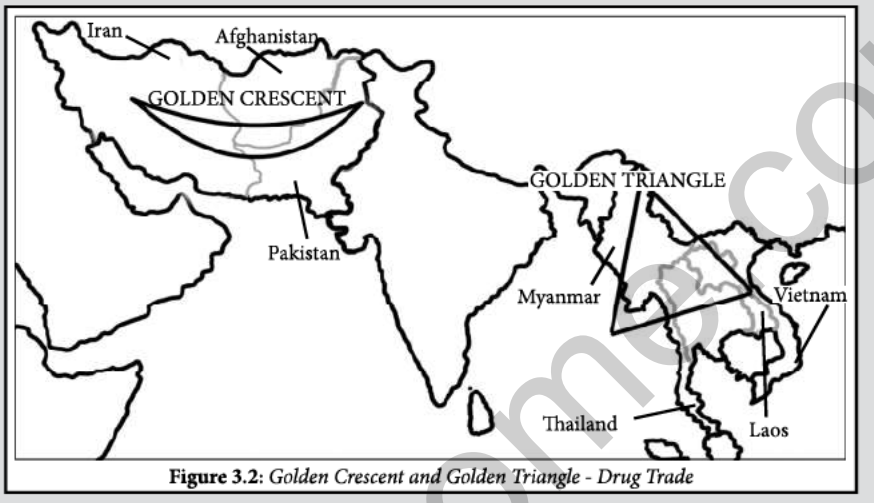


Figure 3.2: *Golden Crescent and Golden Triangle - Drug Trade*

Golden Crescent: The Golden Crescent is the name given to one of Asia's two principal areas of illicit opium production located at the crossroads of Central, South, and Western Asia. This space overlaps three nations, Afghanistan, Iran, and Pakistan whose mountainous peripheries define the crescent.

Golden Triangle : The Golden Triangle is the area where the borders of Thailand, Laos, and Myanmar meet at the confluence of the Ruak and Mekong rivers. This was the highest opium producing region in 1950s until Afghanistan surpassed it.

activities: drug trafficking and terrorist violence. Narco-terrorism is motivated mainly by economic reasons as it helps the terrorist organizations raise huge sums of money with minimum operational cost. Narco-terrorism is a concept, which finds itself in the category of either 'types of Terrorism' or 'means of Terrorism', depending on how it is defined. Though initially used in the context of drug trafficking-related terrorism in South America(Peru), the term has come to be associated with terrorist groups and activities in particular to the Central and South-East Asia because this region has become the hotbed of narcotics production infamously the **Golden Crescent and Golden Triangle. Major terrorist groups** operating on these lines are (a)Al Qaeda, (b) the Colombia-based AUC (United Defences of Columbia), ELN (National Liberation Army) and FARC (Revolutionary Armed Forces of Colombia), (c) Hezbollah in Lebanon, (d) Taliban in Afghanistan and (e) the RIRA (Real Irish Republican Army) in Northern Ireland. Islamist terrorist groups in India supported by the Pakistan ISI are reported to be active in drug trafficking along the Kashmir Valley and also in other parts of the country, for example, Lashkar-e-Taiba, Jaish-e-Mohammad etc.

3.2.3. Factors Behind Terrorism

The **study of terrorism** is debated around explaining what constitutes terrorism and is focussed on short-sighted measures to counter it instead of perhaps analysing the causes behind it. The reasons for people resorting to terrorist activities are complex and based on overlapping causes. The factors cannot be categorised in water tight compartments as they all come together to cause birth of terrorism. Therefore, it is consensually agreed that **terrorism is a long process** and one of the political strategies selected from among a range of other peaceful options to achieve their goals. The process of terrorism has a historical background, which involves people who think that the present political system has alienated them.

One of the major cause of terrorism is **religious fundamentalism and radicalism**. **Religion** is treated to be the most significant among the other causes of terrorism. Fundamentalists and conservatives reject changes which they consider threat to their religion and try to establish an old order by force and indoctrination. Presently, Islamic fundamentalism has been attributed as the major example of religion-based terrorism even though

other forms of terrorism prevail. The terrorist attacks having basis on religious ideology are more dangerous in nature than other types of terrorism. The most prominent example of terrorist attack is of the 9/11 attacks, USA in which the people involved in the attack were migrant Muslims, who went to Germany for their education but were indoctrinated to carry out the attacks. For example, ISIS's religious appeal attracts the unemployed disoriented youth by saying that they would be rewarded for their acts by God after their death. In India, out of the other causes, religion has come out to be the major reason for terrorist activities. In Punjab, some Sikh groups chose terrorism to demand for an independent state called Khalistan based on Sikh religion. In J&K, Muslims belonging to different organisations chose terrorism and support Proxy war of Pakistan as a means for the creation of an independent Azad Kashmir.

Segregation in society based on **religious and ethnic lines** leads to feelings of discontent and alienation in some communities. They believe that their needs and demands are different from other communities or sections of society. There is a general consensus that the government does not pay heed to their needs and they suffer gross social and economic injustice. Sometimes, they also suffer religious persecution from their own countries and have to resort to asylum and become refugees for life. The **Arakan Army** of Myanmar is one such example.

The Arakan Army: The Arakan Army is revolutionary armed organization based in the state of Arakan, Myanmar. Founded on 10 April 2009, the AA is the armed wing of the United League of Arakan (ULA). The Arakan Army purportedly advocates for self-determination for the multi-ethnic Arakanese population, safeguarding and promotion of the national identity, cultural heritage, 'national dignity' and best interests of the Arakan people.

The ethnic and religious communities **face discrimination, alienation and persecution in the society** which leads to the creation of fault lines and unrest. Due to historical injustices and perpetuation of poverty and deprivation over decades, they score low in per capita income and other human development indicators. People who face **excessive poverty** and generally feel deprived from access to economic resources are easily motivated to take part in terror activities in return of monetary benefit. The most important factor of terrorism is disparity in the distribution and access to resources. Approximately, 15% of the world population uses 85% of the total resources. The statistics on economic inequality show that the situation is **grave in developing countries**.

Factors like unemployment, exploitation of landless by landowners and absence of land reforms are the main causes of support to terrorism. The economic grievances and gross social injustice have given rise to ideological extremist groups like the **Maoists**. The differences in income and quality of life between the countries of first world and third world leads to humiliation, frustration, and victimisations in group of people belonging to poor and underdeveloped countries This makes deprived people a potent terrorist recruit by non-state actors who exploit the feeling of discontent already present in the community. The same was seen in the case of terrorists of **Mumbai 26/11 attacks**, who belonged to economically deprived sections of the society.

The other case is of people belonging to different countries and ethnicity **immigrating** to other countries- usually developed or having better opportunities for employment or education and face discrimination from the original residents of the countries. These groups may feel alienated and socially excluded. Such people are easy recruits for terrorist activities and eventually convinced to provide support for technical and logistical requirement of the terrorist organisations.

Inequality in political representation, no voting rights, non-recognition of human and cultural rights of the ethnic or religious minorities, **lack of freedom of religious expression** are some of the major political reasons behind people resorting to terrorist activities. The biased policies of the ruling government or rule of one particular political party having contempt towards particular minority ethno-religious community, lack or inadequate political representation in decision making bodies, barring people from joining positions of authority lead to discontent and piling up of grievances against the other party or sections of society.

The inadequately represented group demands regional independence and self-determination. The Left- and Right-wing terrorists are the example of this type of terrorism. The groups like LTTE and extremism in **Sri-Lanka** was having genesis in political injustice suffered by the ethnic Tamil Groups.

Technological advancement specially in communication sector and greater technological penetration even in remote underdeveloped regions has helped in the spread of terror activities. **Social media platforms** are one of the most widely used medium by terrorist organizations to communicate with people residing in far-flung areas and another country. They are recruiting youth through indoctrination and dissemination of fundamentalist and radical ideas. The Jihadist network spread their propaganda through internet and dark web leading to 'cyber- radicalisation' . This was seen when ISIS recruiters used Facebook to brainwash Muslim youths and align with their ideology of Islamic Caliphate. Those who couldn't join the ISIS in Syria got inspired by the terror group's ideology to commit lone wolf attacks. There were **mass shootings in the USA and attacks in parts of Europe which were categorised as lone wolf attacks**. Deepfakes is another technology, if fallen in the hands of terrorist organisations ,can cause havoc. False videos of war, crime and attacks can incite more violence and problems of law and order.

Lone wolf attacks: The term 'lone wolf' is used by law enforcement agencies and the media to refer to individuals undertaking violent acts of terrorism **outside a command structure**. A lone actor, lone-actor terrorist, or lone wolf is someone who prepares and commits violent acts alone, outside of any command structure and without material assistance from any group. They may be influenced or motivated by the ideology and beliefs of an external group and may act in support of such a group. There have been numerous incidences of lone wolf attacks like the knife attack in a park in Reading, west of London and in 2017, Khalid Masood, a British citizen **drove a car into pedestrians** on the pavement of Westminster Bridge and stabbed a police officer.

Deepfake: It constitutes fake content, often in the form of videos but also other media formats such as pictures or audio, created using powerful artificial intelligence tools. They are called deepfakes because they use deep learning technology, a branch of machine learning that applies neural net simulation to massive data sets, to create fake content.

3.3. MEANS OF TERRORISM

The **conventional** tactics employed by terrorists are attacks on persons and property using weapons, bombs, IEDs, grenades, landmines etc., taking hostages, **hijacking of airplanes** and forcible take-over of buildings especially Government or public buildings. In the recent decades, **fidayeen and suicide attacks**, suicide bombings and kidnapping of journalists, public servants and government officials have also been witnessed. Some unconventional or emerging methods are acquiring Weapons of Mass Destruction (nuclear, chemical or biological), cyber terrorism and environmental terrorism.

Hijacking of IC 814: On 24 December 1999, Indian Airlines flight IC 814 took off from Kathmandu, Nepal, with Delhi, India as its intended destination. The flight left with 180 persons on board, including both the crew and the passengers. It was hijacked mid-flight and went through various locations before landing at Taliban controlled Kandahar airport The motive for the hijacking apparently was to secure the release of Islamist terrorists held in prison in India. The hostage crisis lasted for seven days and ended after India agreed to release three terrorists – Mushtaq Ahmed Zargar, Ahmed Omar Saeed Sheikh, and Masood Azhar. The three have since been implicated in other terrorist actions, such as the 2002 kidnapping and murder of Daniel Pearl and the 2008 Mumbai terror attacks.

In the recent history of terrorism, **suicide attacks** have been the most ominous aspect of the terrorist activities. The first instance of **suicide terrorism** took place in 1984 when US Marine barracks in Beirut were attacked by a vehicle-borne suicide bomber. LTTE also got inspired leading to an LTTE cadre driving a truck filled with explosives

into the Sri Lankan Army camp in Jaffna in 1987, marking the beginning of LTTE's suicide bombing method of creating terror. The assassination of ex- PM Shri Rajiv Gandhi took place on May 21, 1991 which brought into focus the capability and ruthless brutality of LTTE in suicide terrorism. The LTTE has consistently been able to find large numbers of volunteers from amongst Sri Lankan Tamils to carry out suicide missions. The LTTE use mythological and historical stories specially from Silappadikaram, a stirring tale of the **woman warrior Kannagi.**

In Kashmir, Jihadi terrorists took to suicide terrorism in the 1990's. The first suicide attack by the **Fidayeen** was in 1991 on a Border Security Force Post. The attack on the J&K Legislative Assembly complex in October 2001, in which the driver of the explosive-laden vehicle rammed through the gate. Since then, the Fidayeen have been involved in attacking the Indian Parliament in 2001, in storming the Akshardham Temple in Gujarat in 2002 and in an abortive attempt at Ayodhya in July 2005. The 2019 attack on CRPF convoy in Pulwama was the deadliest in recent years which was carried out by a suicide bomber who rammed the explosives laden truck into the convoy leading to death of 40 CRPF personnel. The attack in the Kabul airport during the 2021 Afghanistan crisis was also conducted by suicide bombers of ISIS- Khorasan.

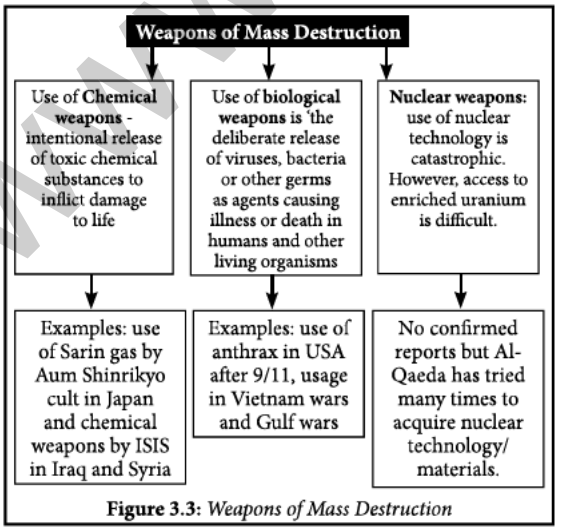


Figure 3.3: *Weapons of Mass Destruction*

Weapons of Mass Destruction (WMD) are the weapons that can inflict heavy damage on a given target. Nuclear, chemical and biological weapons are the commonly identified weapons of mass destruction. Although the term WMD has been in use for a long time, the possibility of acquisition of such weapons by terrorist organizations, the perceived Iraqi possession of it and the US led war on Iraq brought WMD into focus.

Cyber-terrorism is defined as 'the purposeful or threatened use of politically, socially, economically or religiously motivated cyber warfare or cyber-targeted violence, conducted by a non-state or state-sponsored group for the purposes of creating **fear, anxiety, and panic in the target population,** and the disruption of military and civilian assets.' Thus, cyber-terrorism is the most advanced means of terrorist strategy developed with the advancement in information and communication technologies that enables terrorists to carry out their operations with minimum operational costs. Examples include, attack on Estonia in 2007, leading to **Denial of Service (DoS)** and rendering the entire country offline and shutting of essential services. In October 2000, some Israeli youngsters launched DoS (Denial of Service) attacks against the computers maintained by the terrorist groups in Palestine and this was reciprocated by attacks on websites belonging to the Israeli Parliament, Defence Forces, the Foreign Ministry and the Bank of Israel. A series of powerful cyber-attacks on 27 June 2017 swamped websites of Ukrainian organizations, including banks, ministries, newspapers and electricity firms.

Environmental terrorism is the **intentional damage** caused to nature and environmental resources to deprive the others of their use. For instance, on the orders of Saddam Hussein **several oil wells were ignited** to cover Kuwait in smoke during the **Gulf War I**. Similarly, during Gulf War II, the forces of Hussein retreated, set ablaze all oil wells so as make them unusable for the NATO forces. Incendiary balloons from the Gaza Strip were used to burn down approximately 2,260 acres of woodland in Israel in 2018. Children of Fire Initiative, an organization believed to be an offshoot of PKK (Kurdistan Workers Party) claimed responsibility for multiple arson and wildfire attacks in Turkey, including those which happened in 2020.

3.4. TERROR FINANCING

Terror Financing is the **'lifeline'** of Terrorism. Terrorist organisations majorly finance their activities with the help of cartels involved in

organised crimes such as drug and human trafficking, smuggling etc. Counterfeiting of currency, black money, hawala transactions are also few ways to generate funds for terrorist activities. Terrorist organisations also resort to malafide business activities like the ISIS selling oil and gas to other countries at very cheap rates, trafficking of girls to be sold off for prostitution. The source of funds could be the proceeds of illegal operations like enumerated above or even lawful activities. The funds are also collected either through **Ideological patronage** or organised criminal activities. In Ideological Patronage, supporters of an extremist and militant ideology make financial contributions to terrorist organizations from their known sources of income. Such contributions, sometimes are also made to some non-profit or charitable institutions acting as a front for terrorist organizations.

3.5. IMPACTS OF TERRORISM

The ex- Secretary General of UN Ban Ki Moon has said that "Terrorism is a **significant threat** to peace and security, prosperity and people." Terrorism has wide impacts on the individual, community, society, country and the entire world.

Terrorist activities results **in instability in governance** and government authority in the region afflicted by terrorism. The killing of ex-Prime Ministers of India, Mrs Indira Gandhi and Mr Rajiv Gandhi, affected Indian politico-economic situation greatly. The political instability has **impact on foreign relations and prospects of Foreign Direct Investment**. Also, **loss of trust** in the government and authorities in the aftermath of acts of terror is generally witnessed.

Linkages between terrorism and organized crime are convoluted and multitudinous, resulting in a serious threat to not only national peace but also international stability. Their interactions are based on shared interests. Terrorists derive benefit from organized crime, together with trafficking in persons and migrant smuggling, trafficking in drugs, firearms, cultural property etc. Organized crime groups are also involved in relocating terrorists across the border. **26/11 attacks in Mumbai** are a perfect example of how organized crime networks and terrorist organizations work in **cohort** of each other. Then the D-Company led by **Dawood Ibrahim** provided all the logistical support to the terrorist for carrying out their activities. Terrorist organizations in turn are a great **paymaster** to the organized crime networks. Thus, the two share a **diabolical symbiotic relationship**.

Hawala Transactions and Terror Financing

In a hawala transaction, no physical movement of cash is there. It is an alternative or parallel remittance system, which works outside the circle of banks and formal financial systems. As hawala transactions are not routed through banks they cannot be regulated by the government agencies and have thus emerged as a major cause of concern as it is frequently used by criminals to launder money for their illicit act. This network is being used extensively across the globe to circulate black money and to provide funds for terrorism, drug trafficking and other illegal activities. Hawala system works with a network of operators called 'Hawala Dealers'. A person willing to transfer money, contacts a Hawala operator at the source location who takes money from that person. The Hawala operator then calls upon his counterpart at the destination location who gives the cash to the person to whom the transfer has to be made, thus completing the transaction. Hawala is illegal in India, as it is seen to be a form of money laundering. As hawala transactions are not routed through banks, government agencies and the RBI cannot regulate them. In India, FEMA (Foreign Exchange Management Act) 2000 and PMLA (Prevention of Money Laundering Act) 2002 are the two major legislations which make such transactions illegal.

Cryptocurrencies used for Terror Funding

Terrorists are increasingly resorting to newer technological tools and social media. The justice department of the USA in 2020 said that it dismantled an elaborate cyber campaign used by overseas terror organizations to finance their operations. 2 million USD were seized from more than 300 cryptocurrency accounts. Terrorist groups like ISIS, used cryptocurrency and social media to raise funds for their terror campaigns.

The relationship between state and its people gets disrupted as citizens lose faith in the authority as protector of the sovereignty and dignity of the nation. Governance suffers as communication lines and **physical infrastructure is damaged**. The post attack decisions mostly centre on strengthening the security and intelligence aspect and diversion of funds takes place ignoring the developmental needs of the vulnerable section.

The social impact of terrorism is very far-reaching as it influences many different aspects of society. Terrorism impacts the beliefs and attitudes of the people, influencing their opinion either in favour or against depending on which side they belong to. Terrorism leads to creation and deepening of group divide and reduced trust of citizens in the institutions of the state as well as in other fellow citizens. Due to this, the **communal identity** solidifies. **In- group and Out-group classification** becomes prominent where people from different groups and communities see each other with suspicion and apprehension. Feelings of Ethno- centrism and Xenophobia increase post attack. The society becomes generally intolerant towards other communities and ethnicities which disrupts the **secular and social fabric** of the nation.

The impact of terrorism and war is always **negative for the economy**. **Large scale physical destruction** leads to the loss of productive resources that might have generated valuable goods and services. The victim country finds itself at the crossroads to invest in defence or developmental schemes eventually leading to increased spending on defence and security. The 26/11 terrorist attack in Mumbai greatly impacted the investor sentiment and affected tourism, hospitality and other industries. The stock markets in India were down after the terror incident. The domestic and foreign investment reduces, impacting the employment opportunities of the people. The most immediate and measurable impact of terrorism is physical destruction of infrastructure. Terrorists destroy existing buildings, plants, machines, transportation systems and other economic resources. The attack on the World Trade Centre on Sept. 11, 2001 destroyed billions of dollars' worth of property and killed thousands of productive workers.

According to the **Global terrorism Index**, the global economic impact of terrorism was estimated to be US$26.4 billion in 2019. This is 25 per cent less than the prior year and the fifth consecutive year that it has declined. The improvement over the last four years is largely driven by the declining level of terrorism in Iraq, Nigeria, Pakistan and Syria. Since its peak of $116 billion in 2014, the economic impact has decreased by 77 per cent reflecting the reduction in terrorism deaths, injuries and attacks globally. In the 11th BRICS Summit in Brazil, **Prime Minister Modi** said terrorism has emerged as the biggest threat to the development, peace and prosperity and it caused a **$1 trillion loss to the world economy**.

Terrorism impacts the economy and sectors specially the service sectors. It disrupts dissemination of services and hospitality sectors. The areas afflicted by disturbances and terrorist activities get no tourists and the hospitality sector sees a slump. The effects extend outside to activities directly associated with tourism, like hotels, catering, airlines, and other sectors. To understand the impact, Reuters reported that it expected a 30% decline in visitors to France in the month after the **Nice terror attacks** which is otherwise preferred as a famous tourist destination. In India, Jammu and Kashmir was a famous tourist destination but terrorism damaged its prospects badly. In 2016, Tourist arrivals had gone **down from 12,000 to 250 per day and hotel occupancy was around 3 per cent**, due to increased terrorist activities.

26/11 attack : The 26/11Mumbai attacks were a series of terrorist attacks that took place in November 2008, when 10 members of Lashkar-e-Taiba, an Islamist terrorist organisation from Pakistan, carried out 12 coordinated shooting and bombing attacks lasting four days across Mumbai. The attacks, which drew widespread global condemnation, began on Wednesday 26 November and lasted until Saturday 29 November 2008. At least 174 people died, including 9 attackers, and more than 300 were wounded.

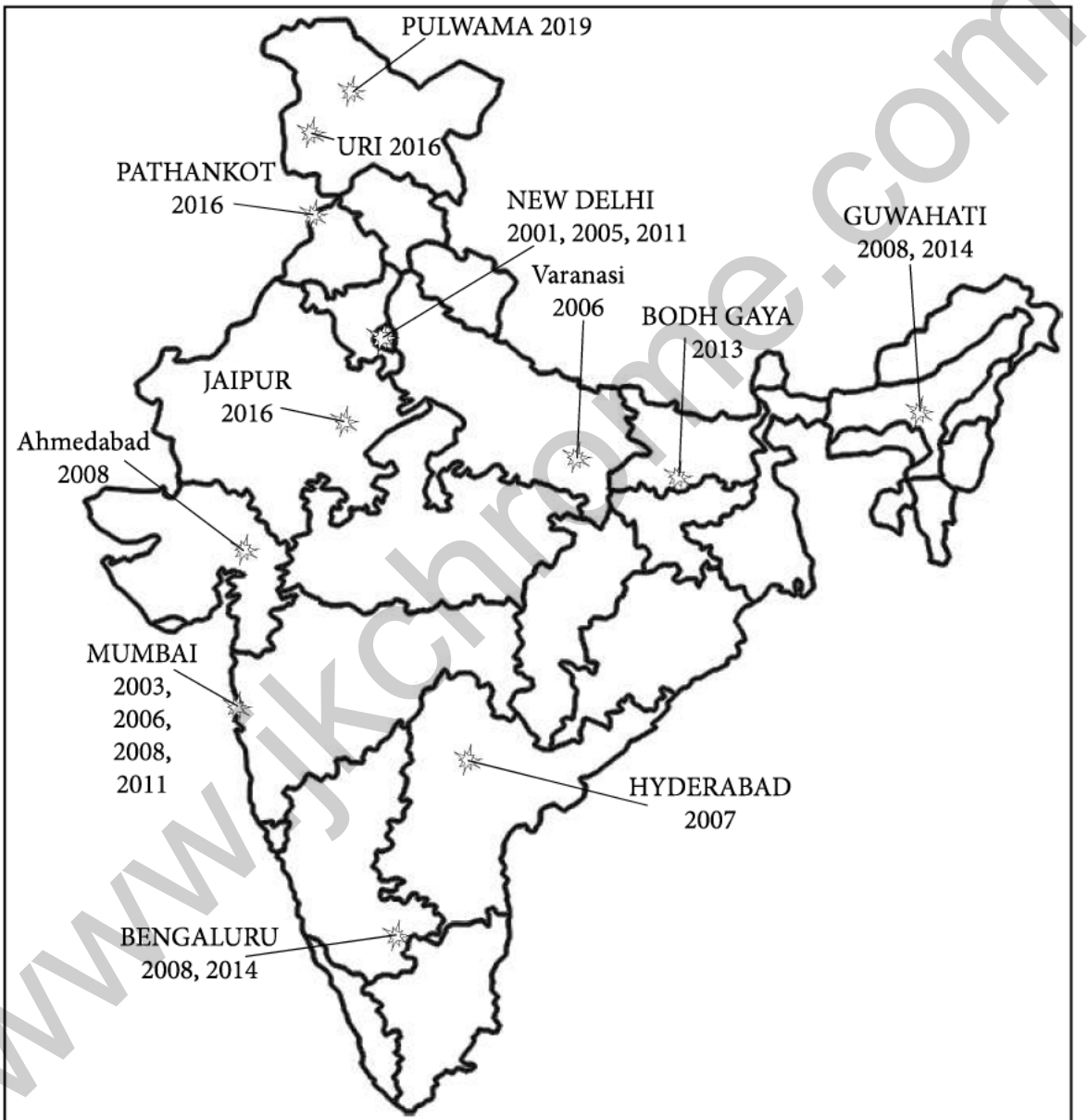


Figure 3.4: *Major Terrorist Attacks in India*

3.6. CHALLENGES IN DEALING WITH TERRORISM

Terrorism is a complex issue as the underlying causes are interconnected and have wide impact. To deal with it is a mountainous task daunting the government and authorities all around the world. The major challenge is that at present there is **no clear definition** of terrorism as it is believed that one man's terrorist is another man's freedom fighter. There is no consensus on the definition of terrorism at the global level. This hampers global coordination on terrorism. It is also a 'transnational issue' as terrorists of one country can be considered as heroes or freedom fighters in adjoining regions or other countries. Thus, it becomes very challenging to curb terrorism when terrorist organisations get support from other countries. **Absence of cooperation** between countries is another factor. Some countries have their state policy of **'Proxy War'** against their neighbour. Such policies can be both explicit and implicit as seen in Pakistan's

policy of **bleeding India through a 'thousand cuts'**. Many countries support through finance and technology, giving shelter on their soil which makes fighting terrorism a difficult task. Drug trafficking, smuggling finances the terrorist organisations leading to deep linkages between organised crime and terrorism.

Terrorism is not just a law-and-order problem but its roots lie in **'Ideological fight'** and decades of deprivation. In the present times, rapid spread of misinformation through social media and internet affects the thinking and generates prejudices in the minds of the people. They take up arms, get involved in illegal activities to avenge the injustices suffered by the people of their community. Rooting out terrorism requires dealing with it on the ideology level too. Isolated episodes of communal riots, lynching incidents leads to radicalisation of youth. They are indoctrinated against state by the fundamentalists which leads to loss of human capital and demographic dividend. Social media has acted as an added tool in the hands of terrorist organization for spreading their communal agenda. ISIS is a case in point. The Islamic State aka Islamic State of Iraq and the Levant or the Islamic state of Iraq and Syria is an Islamic militant jihadist group and a former unrecognized proto state that follows a Salafi jihadist doctrine based on the Sunni branch of Islam. Its genesis can be traced back to the aftermath of the Iraq war. Recently, ISIS claimed the responsibility of the attack on a mosque in Pakistan. ISIS has been at the forefront of employing social media to extend its agenda. It actively carries out radicalization camps in social media. For example, 21 people, including women and children, from the southern State of Kerala went missing in 2016, after falling prey to ISIS propaganda on social media. Also, ISIS has actively used online platforms for conducting virtual training camps. Such misuse of social media platforms can become an added threat to India's internal security. Further, it has posted many beheading videos on various social media platforms in order to spread terror in the minds of people. Such videos have the tendency to instil fear and insecurity in the minds of the masses.

To deal with terrorism, a lot of country's economic resources are used which reduces the financial capacity of the state, leading to less availability of funds for developmental purposes. Huge manpower is dedicated for intelligence gathering and analysis, thwarting threats, ensuring security and law and order which requires significant budgetary expenses.

Q. Religious indoctrination via social media has resulted in Indian youth joining the ISIS. What is ISIS and its mission? How can ISIS be dangerous to the internal security of our country. **(UPSC 2015)**

3.7. IDEA BEHIND COUNTER TERRORISM

Prevent To stop people becoming terrorist or supporting terrorism	**Pursue** To stop terrorist attacks
Protect To strengthen our protection against a terrorist attack	**Prepare** To mitigate the impact of a terrorist attack

As every terrorist organisation has different motives and ideologies, one single approach or strategy cannot be considered as the solution to terrorism. Terrorism has many forms and is based on various complex interconnected reasons; therefore, counter terrorism also needs to be comprehensive. Counter-terrorism policies have to be holistic and multi-pronged including all aspects - social, political, legal and economic. It has to be assimilated in the overall context of national security strategy rather than viewing it narrowly as just terrorism.

The protection of life and property has dominated the discussion of issues of national security but it needs to be considered that a meaningful secure environment is possible only when it factors in socio-economic development of all and in particular the vulnerable communities. Poverty and deprivation is one of the major causes and the breeding grounds for terrorism. The deprived and alienated sections of the society fall victim to the terrorist propaganda and misinformation. The best strategy is to bring about overall inclusive socio-economic development.

The tussle between centre and state should be resolved to streamline cooperation in matters of

intelligence sharing. There should be open frank two-way communication in matters of security. Political parties should rise above petty politics and vested interests to assure people of **good governance and sustainable development**. The administration should become sensitive to the needs and grievances of the citizens and the service delivery methods should be made prompt in response. Along with this, the Justice system and the Law Enforcement Agencies have to be overhauled and supported with the sound legal framework, training infrastructure, advanced equipment and intelligence support. Developmental schemes and policies should be implemented in letter and spirit to achieve good governance. Corruption, nepotism and other evils should be eliminated. Transparency and accountability in governance should be the ethos when serving people.

Counter terrorism is not **routine law enforcement** but requires special skills of **coordination and intelligence**. The police forces are overburdened and overstretched with their routine work and it is not possible for them to dedicate time and energy for counter terrorism. A **specialised force** is required to deal exclusively with terrorism but they need to work in tandem with the local police and ground intelligence. The approach should be integrated having the involvement of all the stakeholders, the government, political parties, security agencies, civil society and media.

3.8. INDIA'S STEPS TOWARDS COUNTER TERRORISM

3.8.1. Legislative Measures

India has framed laws through the **legislative route** to tackle terrorism and unlawful activities. Terrorism as an offence does not figure in the Indian Penal Code of 1860, hence separate laws have been framed time and again to deal with it effectively. In India, the first special law which attempted to define terrorism was the TADA :Terrorist and Disruptive Activities (Prevention) Act, 1987, which was followed by the Prevention of Terrorism Act, 2002 (**POTA**). With the repeal of the latter in 2004, the **Unlawful Activities (Prevention) Act, 1967** was amended to include the definition of a 'terrorist act'.

Terrorist and Disruptive Activities (Prevention) Act, 1987 was an **anti-terrorism law** which was in force between 1985 and 1995 in the background of the **Punjab insurgency** and was applied to whole of India. It was the first anti-terrorism law legislated by the government to define counter-terrorist activities. Due to heavy criticism of the Act , it was allowed to lapse in 1995. After that the **Prevention of Terrorism Act, 2002 (POTA)** was passed by the Parliament of India in 2002, with the objective of strengthening anti-terrorism operations. The Act was enacted due to several terrorist attacks that were being carried out in India and especially in response to the attack on the Parliament. The Act was repealed in 2004 due to allegations of misuse by the state governments. **The Unlawful Activities (Prevention) Act, 1967 was amended in 2004,** to include the definition of **'terrorist act'** which says:

1. whosoever, with intent to threaten the **unity, integrity, security or sovereignty** of India or to strike terror in the people or any section of the people in India or in any foreign country,
2. does any act by using bombs, dynamite or other explosive substances or inflammable substances or firearms or other lethal weapons or poisons or obnoxious gases or other chemicals or by any other substances (whether biological or otherwise) of a hazardous nature, in such a manner as to cause, or likely to cause, death of, or injuries to any person or persons or loss of, or damage to, or destruction of,
3. property or disruption of any supplies or services essential to the life of the community in India or in any foreign country or causes damage or destruction of any property or equipment used or intended to be used for the defence of India or in connection with any other purposes of the Government of India, any State Government or any of their agencies
4. or detains any person and threatens to kill or injure such person in order to compel the Government of India or the Government of a foreign country or any other person to do or abstain from doing any act, commits a terrorist act.

2001 Parliament Attack: The 2001 terrorist attack was targeted on the Parliament of India in New Delhi on 13 December 2001. The perpetrators belonged to Lashkar-e-Taiba (LeT) and Jaish-e-Mohammed (JeM) - two Pakistan-raised terrorist organizations. Though no legislator/parliamentarian lost his life the attack led to the deaths of six Delhi Police personnel, two Parliament Security Service personnel, and a gardener. It led to increased tensions between India and Pakistan, resulting in the 2001–02 India -Pakistan standoff. Four people were held to be guilty, out of which two were sentenced to death. The trial and death sentence given by the court to one of the accused, Afzal Guru created quite an uproar.

3.8.1.1. National Investigation Agency Act 2008 (Amended in 2019)

The National Investigation Agency is an **apex anti-terror agency**, thoroughly professional and investigative agency matching the best international standards. The NIA aims to set the standards of excellence in counter terrorism and other **national security related investigations** at the national level by developing into a highly trained, partnership-oriented workforce. NIA aims at creating **deterrence** for existing and potential terrorist groups/individuals. It aims to develop as a storehouse of all terrorist related information. Under the National Investigation Agency Act, the NIA can investigate offences under Acts such as the **Atomic Energy Act, 1962,** and the **Unlawful Activities Prevention Act, 1967**.

Provisions of NIA(2019 Amendment)

1. It **expanded the type of offences** that the investigative body could investigate and prosecute. The agency can now investigate offences related to human trafficking, counterfeit currency, manufacture or sale of prohibited arms, cyber-terrorism, and offences under the Explosive Substances Act, 1908.
2. The amended bill gave NIA officers the power to **investigate offences committed outside India**. However, NIA's jurisdiction will be subject to international treaties and domestic laws of other countries.
3. The amendment also enables the central government to **designate sessions courts as special courts** for NIA trials.
4. It also allows an NIA officer to **conduct raids, and seize properties** that are suspected to be linked to terrorist activities without taking prior permission of the Director General of Police of a state. The investigating officer only requires sanction from the Director General of NIA.

Issues with the 2019 Amendment in NIA Act:

The Chhattisgarh government moved Supreme court in 2020 stating that the NIA act was ultra vires to the constitution and outside the legislative competence of the Parliament. According to the state, the 2008 Act allows the Centre to create an agency for investigation, which is a function of the state police. 'Police' is an entry in the State List of the Constitution's 7th Schedule. The Act takes away the state's power of conducting an investigation through the police, while conferring 'unfettered, discretionary and arbitrary powers' on the Centre.

3.8.1.2. Unlawful Activities Prevention Act, 1967 (Amended in 2019)

It is **primarily an anti-terror law** aimed at effective prevention of certain unlawful activities of individuals and associations. Its main objective is to empower the state for dealing with activities **directed against the integrity and sovereignty** of India. The Act assigns absolute power to the central government. It can declare any activity as unlawful, by way of an Official Gazette.

2004 amendment: It added **'terrorist act'** to the list of offences, to ban organisations for terrorist activities. Till 2004, 'unlawful' activities referred to actions related to secession and cession of territory. Following the 2004 amendment, the 'terrorist act' was added to the list of offences.

2019 amendment: The amendment empowers the Central Government to **designate individuals as terrorists** on certain grounds. It empowers the Director-General, National Investigation Agency (NIA) to grant approval of seizure or attachment

of property when the case is under investigation by the agency. It also empowers the officers of the NIA, of the rank of **Inspector or above, to investigate cases of terrorism**. Earlier, the power to investigate was with the officers of the rank of Deputy Superintendent or Assistant Commissioner of Police only.

Criticisms associated with UAPA : The UAPA has faced criticism due to certain draconian provisions as highlighted by critics and experts, where foremost the definition of terrorism is indefinite and comprehensive covering all violent acts. Some of the other issues are:

Firstly, the wide provisions of the act have been used by the government to curb political dissent rather than to protect sovereignty and integrity. Recently, Justice D Y Chandrachud also said that the stringent UAPA law should not be misused to quell dissent.

secondly, the principle of natural justice calls for assuming every person innocent unless proven guilty and hence a pre-trial imprisonment is a violation of this principle. The UAPA allows the Court to deny bail for a terrorist act if there are reasonable grounds to believe that the accusation is prima facie true.

Thirdly, The wide powers given to police for search and arrest is a clear violation of an individual's right to privacy. It is a fundamental right under Article 21 of the Indian constitution as deduced by court in K.S Puttaswamy versus Union of India.

Fourthly, some experts feel that it is against the federal structure since it neglects the authority of state police in terrorism cases.

Fifthly, the wide and ambiguous provisions of the act enables the state to impose frivolous charges on innocent individuals. This is testified by a mere 2.2% conviction rate under UAPA between 2016-2019.The total number of persons arrested and convicted under UAPA was 5,922 and 132 respectively.

Lastly, the NCRB does not maintain UAPA data on the basis of religion, race, caste or gender. This creates a barrier in identifying the vulnerable groups who face greater abuse under the act.

Q. Indian Government has recently strengthened the anti-terrorism laws by amending the unlawful Activities (Prevention) Act (UAPA), 1967 and the NIA act. Analyze the changes in the context of prevailing security environment while discussing the scope and reasons for opposing the UAPA by human rights organizations.**(UPSC 2019)**

3.8.2. Institutional Measures

The major role of anti-terrorist agencies in India is **'intelligence gathering'.** The primary role of intelligence collection is played by the state police and the central government agencies. **NATGRID** and **MAC** (Multi-Agency Centre) formed after **26/11** have been instrumental in being a force multiplier. **NATGRID** is an integrated intelligence grid connecting databases of core security agencies to collect comprehensive patterns of intelligence that can be readily accessed by intelligence agencies. The database would be accessible to authorised persons from 11 agencies on a case to case basis and only for professional investigations into suspected cases of terrorism. It will utilize technologies like Big Data and analytics to study and analyse the huge amounts of data from various intelligence and enforcement agencies to help track suspected terrorists and prevent terrorist attacks.

MAC (Multi-Agency Centre), headquartered in New Delhi is a common counter-terrorism grid under the **Intelligence Bureau.** It was made operational in 2001 following the Kargil War. It is working as the 24/7 nodal agency for the exchange of intelligence collected by various agencies and police forces across the country. As many as 28 organisations, including the Research and Analysis Wing (R&AW), armed forces and State police, are part of the platform. Various security agencies share **real-time intelligence inputs** on the MAC. MAC coordinates with representatives from numerous agencies, different ministries, both central and state. The state capitals have subsidiary MACs(SMACs) where daily meetings are held to analyse inputs received in the previous 24 hours. Due to the reluctance of the states to share intelligence, recently, the Central government has asked them to share more intelligence inputs through MAC.

But the collection of information and vital inputs from other government departments and other non-government bodies like information regarding fake currency, smuggling, cross border infiltration, financial details etc. still need to be streamlined so as to facilitate exposure of terror threats.

The **capacity building** of the intelligence agency and paramilitary forces is not on the required lines. Training opportunities and availability of new equipment for the state police forces have been limited. Major scope for improvement exists as only forces like the central forces (CAPF) have been getting attention towards modernisation only since past few years. Intelligence Bureau(IB) plays the role of coordinator with the police belonging to different states but in case of some multistate operation, there is absence of unified command.

The next most important step is of **conducting investigations**. The organisational efficiency should be improved to deal with issues related to the investigation. For this purpose, NIA (National investigation agency) was created. One unified central agency like NIA which investigates all such cases of terrorism which are inter-linked and occur in different states offers efficiency. (Security agencies have been covered in detail in security forces and agencies and their mandate chapter)

3.8.3. Border Management

In the aftermath of the **Pathankot attack**, the government had approved a plan to stop infiltration over 2900 kilometres western border with Pakistan under the name **Comprehensive Integrated Border Management System** (CIBMS).Important component of the CIBMS is the use of **satellite imagery,** which would help the security forces to find out details of the terrain and fortifications across the border. It would also help in planning operations and for infrastructure development. Also, **BOLD-QIT** ***Border Electronically Dominated QRT Interception Technique*** is the project to install technical systems under the Comprehensive Integrated Border Management System (CIBMS), which enables BSF to equip Indo-Bangladesh borders with different kinds of sensors in the unfenced riverine area of the Brahmaputra and its tributaries.

Comprehensive integrated Border Management System (CIBMS) involves deployment of a range of state-of-the-art surveillance technologies like thermal imagers, infra-red and laser-based intruder alarms, aerostats for aerial surveillance, unattended ground sensors that can help detect intrusion bids, radars, sonar systems to secure riverine borders, fiber-optic sensors and a command-and-control system that shall receive data from all surveillance devices in real time. Implementation of CIBMS projects on Indo - Pakistan and Indo - Bangladesh border will enhance the capabilities of Border security Force (BSF).

3.8.4. Stopping Terror Financing

The provisions in the **Unlawful Activities (Prevention) Act, 1967** has been strengthened to combat terror financing by criminalising the production or smuggling or circulation of high-quality counterfeit Indian currency. **Terror Funding and Fake Currency** (TFFC) Cell has been constituted in the National Investigation Agency (NIA) to conduct a focused investigation of terror funding and fake currency cases. The Indian government has taken initiatives against Black money through demonetisation and simplifying tax filing procedures. **Remittance procedures have been simplified** by the Central Banks to control Hawala Transactions. The government has taken out various guidelines with the aim to crackdown on NGOs getting illicit foreign funds being used for anti- state activities. Training programmes are regularly conducted for the State Police personnel on issues to combat terrorist financing. Intelligence and security agencies of Centre and States work in tandem to keep a close watch on the elements involved in terror funding activities and take action as per law.

Fake Indian Currency Notes (FICN) network is one of the channels of terror financing in India. **FICN Coordination Group** (FCORD) has been formed by the Ministry of Home Affairs to share intelligence/information among the security agencies of the states/centre to counter the problem of circulation of fake currency notes. Security at the international borders has been strengthened

by using new surveillance technology, deploying additional manpower for round the clock surveillance, establishing observation posts along the international border, erection of border fencing and intensive patrolling. Training programmes are conducted for the Police officials of Nepal and Bangladesh to sensitize them about smuggling/ counterfeiting of Indian currency.

3.8.5. Cybersecurity

Besides enacting cyber legislations, the government has also undertaken organisational measures by establishing new centres for cybersecurity such as the **National Critical Information Infrastructure Protection Centre and the National Cyber Coordination Centre;** creating a division covering Cyber and Information Security within the Ministry of Home Affairs; and improving institutional capacity building through training of personnel and generating awareness. (covered in detail in Cybersecurity chapter)

3.8.6. Countering Propaganda and Developmental Initiatives

Efforts towards **de-radicalisation** of the misguided youth by the state police has given positive results (Telangana model). Initiatives focussing on reassimilation of terrorists and misguided youth into mainstream society with **'Surrender and Rehabilitation' policy** like in the Jammu and Kashmir has also led to good results.

Ministry of Home Affairs has been tasked with the monitoring of **Aspirational districts** programme in 35 LWE affected districts, Kashmir and other backward districts in India which aims to quickly and effectively transform these districts. Employment opportunities, skill development, scholarship schemes have provided more avenues to the youth to shun violence and contribute in the development of the region and the country. Schemes like UDAAN, HIMAYAT etc. have been started to support unemployed and unskilled youth of Jammu and Kashmir UT. Thus, the Government is committed to raising the living standards of its citizens and ensuring inclusive growth for all – "Sabka Saath Sabka Vikas".

Back to village: It is the programme of the Jammu and Kashmir government for reaching out to the people at the grassroots level to create in rural masses an earnest desire for a decent standard of living. The programme is aimed at energizing panchayats and directing development efforts in rural areas through community participation.

3.8.7. International Cooperation for Counter Terrorism

As terrorism is a global problem, solutions have been sought through multilateral agencies like UN. India proposed a draft document on the **Comprehensive Convention on International Terrorism (CCIT)** at the UN in 1986 but it has not been adopted as there is no unanimity on the definition of terrorism among the member states. The other initiatives are **FATF (Financial action task force)** for whom **combating terrorist financing** has been a priority since 2001. It plays a central role in efforts at international level in combating terrorist financing, through its role in setting global standards to combat terrorist financing, assisting jurisdictions in implementing financial provisions of the United Nations Security Council resolutions on terrorism and evaluating countries' ability to prevent, detect, investigate and prosecute the financing of terrorism. The United Nations has launched a new framework titled **'UN Global Counter-Terrorism Coordination Compact'** to combat international terrorism and coordinate efforts across the peace and security, humanitarian, human rights and sustainable development sectors. The framework is an agreement between the UN chief, 36 organisational entities, the International Criminal Police Organisation (INTERPOL) and the World Customs Organisation to better serve the needs of member states when it comes to tackling the scourge of international terrorism. The Coordination Committee of the United Nations will oversee the implementation of the framework and monitor its implementation. The committee will be chaired by UN Under-Secretary-General for counter-terrorism. Along with the above initiatives, diplomatic weight and tactics should be used to build consensus and policy convergence on issues related to terrorism.

CCIT: The **Comprehensive Convention on International Terrorism** is a proposed treaty which intends to criminalize all forms of international terrorism and deny terrorists, their financiers and supporters' access to funds, arms, and safe havens. India proposed this convention in 1996, however, as of 2021 consensus has not been reached for the adoption of the convention. The main reason for the deadlock in convention is because of difference over the definition of terrorism. Indian Prime Minister pushed for the CCIT by reiterating its need during the 69th session of UN General Assembly held in September 2014.

3.9. WHAT MORE CAN BE DONE TO FIGHT THE MENACE OF TERRORISM?

Dealing with terrorism requires a comprehensive approach in which different stakeholders like the government, political parties, security agencies, civil society etc. have an important role to play. The **state police and intelligence network** should be strengthened enhancing their training facilities and ensuring the availability of modern equipment for investigation, surveillance and operations when the time comes. We also need to have modern scientific forensic laboratories so as to have proactive investigative infrastructure available at the disposal of police bodies. Also, due to the advancement of Information technology, cybercrime incidents are rising due to which sophisticated cybersecurity architecture becomes the need of the hour to prevent perpetration of terror, religious indoctrination etc. in the minds of people through social media and Dark web.

Keeping pace with changing faces of terrorism, laws should be modified to remove irrelevant provisions. **New comprehensive laws** can be brought in to address needs of counter terrorism in 21st century. A **no-tolerance policy** towards terrorism should be adopted and implemented. **Stringent laws** should be applied **and fast track courts** should dispose of cases efficiently and in time bound manner. Police forces possess limited powers against terrorists as laws against terrorism are very similar to laws against other crimes. An example can be cited of this issue that the power for detention is only for 24 hours in both circumstances. Also, we need to upgrade and make our **criminal justice system** active as a weak system boldens the terrorist organisations to indulge in violent activities.

Centre and states should continue with their **coordinated efforts** where Centre should play a supportive role with state police forces taking the lead in fighting the menace of terrorism and creating appropriate conditions for the citizens to voice their concern to the authorities. Effective participation of centre and states becomes important because law and order is a state subject and the responsibility to fight against terrorism is the responsibility of both central armed forces and state police. Sharing of intelligence between Centre and state should be streamlined. Government should take necessary steps to **cut sources of terror financing** either originating within country or outside. **Regulation** of cryptocurrencies and digitisation of payment systems will help curtail illicit financing methods. Terror financing is the root evil of all threats and its elimination will help deal with terrorism.

Development is the antidote to terrorism. Education, skill development, employment avenues along with physical and social infrastructure should be prioritised in underdeveloped and remote regions. Mainstreaming the vulnerable sections would help in rooting out terrorism. The **citizens** play an important role in counter terrorism , being the eyes and ears of the local police and law enforcement agencies. Sensitisation, awareness and behavioural modification should be undertaken in security forces to avoid prejudices and subsequent alienation of the people belonging to vulnerable communities and sections. Inter religious and inter community **harmony** should be maintained which highlightes the role of religious leaders in maintaining peace.

Media should exercise self-restraint and should aim towards dispassionate journalism. Media plays an important role in awareness generation and helps mould the thought process and beliefs of the people. Issues of national security should be sensitively discussed and media trials should not be conducted if the matter is sub-judice. Social media platforms should be **self-regulated and monitored**

to rule out indoctrination and radicalisation activities by fundamentalists.

For sustainable development of the country, **stability, good governance** and the rule of law are inter-linked. Any threat to peace and harmony subverts the political and social climate but also threatens the economic stability of the country, **undermining democracy and depriving ordinary citizens** of their rights. Terrorists do not belong to any religion or faith or community. Terrorism is an attack on democracy and the civilized society by few people who resort to targeted killing of innocent citizens in pursuit of their evil designs. In some respects, terrorism is more damaging than an act of war against the nation because terror acts often target innocent civilians, apart from the symbols of the State.

Terrorism today has acquired **newer and more dangerous dimensions** threatening international peace and stability worldwide with the use of modern communication systems and state-of-the-art technology combined with **global linkages with organized crime**, drug trafficking, counterfeit currency and money laundering. That is why international cooperation is essential in the fight against terror. India has been one of the worst victims of terrorism but our society has shown tremendous spirit and resilience in the wake of repeated and wanton terrorist attacks by maintaining communal harmony and social amity. It is time however for the nation to gear itself to counter terror in a more coherent and proactive manner and not rely on the patience of its citizens to outlast and defeat terrorists and their supporters.

Q1. The scourge of terrorism is a grave challenge to national security. What solutions do you suggest to curb this growing menace? What are the major sources of terrorist funding? **(UPSC 2017)**

Q2. "Terrorism is emerging as a competitive industry over the last few decades." Analyze the above statement. **(UPSC 2016)**

Q3. Indian Government has recently strengthened the anti-terrorism laws by amending the unlawful Activities (Prevention) Act (UAPA), 1967 and the NIA act. Analyze the changes in the context of prevailing security environment while discussing the scope and reasons for opposing the UAPA by human rights organizations. **(UPSC 2019)**

Q4. Analyse the complexity and intensity of terrorism, its causes, linkages and obnoxious nexus. Also suggest measures required to be taken to eradicate the menace of terrorism. **(UPSC 2021)**

Linkages of Organised Crime with Terrorism

The links between organized crimes and terrorism represent **a growing threat to our world.** The **convergence of crime syndicates and terrorists,** including in **tactics and resources,** enable them to **gain stronger capacities to disrupt peace**, security, economic and social life and human development.

4.1. ORGANISED CRIME

The **UN convention against Transnational Organised Crime (UNTOC)** does not exactly define organised crime due to its multiple and varying interpretations in different countries. But it defines **'organised criminal group'** as a group of three or more people that was not randomly formed, is existing for a period of time, acts in concert with the aim of committing at least one crime punishable by at least four years' incarceration in order to obtain financial or other material benefits. **Interpol** defines organised crime as "any enterprise or gang of persons engaged in continuing illegal activity which has its primary activities that bring together a client–public relationship which demands a range of goods and services which are illegal." As per **Maharashtra Control of Organised Crime Act, 1999 (MCOCA)**, 'Organised crime' is defined as any continuing unlawful activity by an individual, singly or jointly, either as a member of an organised crime syndicate or on behalf of such syndicate by using violence or threat of violence or intimidation or coercion, or other unlawful means, with the objective of gaining pecuniary benefits, or gaining undue economic or other advantage for himself or any person or promoting insurgency.

The most obvious distinction between organized crime and other forms of criminal conduct is the aspect of being 'organized'. The organized crimes are not random, unplanned, individual criminal acts. The activities under organized crimes are rather structured along a viable - even if illegal and unethical - business model, with a robust organizational structure and well-defined hierarchies which may resemble corporate organizations. The organized crimes are generally performed through syndicates of centralized enterprises run by criminals. These criminal organizations perform planned, rational acts that reflect the efforts of individuals, groups and their network in pursuit of often monetary and sometimes political goals.

4.1.1. Characteristics of Organised Crime

Organized crimes have certain identifiable characteristics. The first one is **continuity.** Continuation of the illegal business through survivorship and succession is practised by most of the criminal organizations. The organizations, gangs or the mafia are structured in a way that they survive sudden changes in leadership or succession. **Structure** is the second most vital characteristic of these groups. The criminal gangs are hierarchical and well-structured. There are sub-gangs who are assigned specific tasks which serves the organisation's objective. The criteria for **membership** are another differentiator. To become a core member of the criminal gang one has to possess similar background like belonging to an ethnic gang or have a criminal background.

The individual should be driven by mutual interest. Loyalty is valued trait among members who are rewarded suitably for it. **Criminality** is a core identifier as the main source of income for these organizations is crime. The criminal organizations and gangs indulge in mostly illegitimate businesses to earn income. The illegitimate businesses include extortion, kidnapping, murder, intimidation, robbery, flesh trade, drug peddling, smuggling, etc.

Violence is legitimate part of the operations. Violence is used as a method to intimidate people into submission. Most of the violence is carried out in open for people to see. The intention is to create an atmosphere of fear in the community about the organization. **Disregard for laws, rules and public order** is at the centre of such organizations' activities. Criminal gangs quite often resort to disturbing public order and tranquillity for in chaos such organizations thrive. Panic among the public is the motive behind such public disorder. The public are harassed with utter disregard for the rule of law. **Monopolisation of trade** is attempted to corner monetary benefits when criminal gangs diversify into more legitimate businesses. The monopolies are established using muscle power and violence. Labour contracts in ports, constructions, sand quarrying, liquor outlet contracts are awarded to such organised gangs as a result, which increase the influence of criminal organisations. Lastly, **corruption** is hand-in-glove with organised crime. The criminals bribe officials, higher officials and politicians so that they carry out their illegal activities without any restraint from government officials or police.

4.1.2. Reasons for Growth and Sustenance of Organised Crimes

The **demands** for **illegal goods** in global market like arms and ammunitions, banned drugs, narcotics generate significant cause for organised crimes to thrive. Trafficking of humans, human organs, organs of endangered wild life for use as traditional medicine etc. are also the areas where the organised criminal groups operate. India's **geographical location** and open porous borders, the proximity with drug producing regions like **Golden Crescent** in the West and **Golden Triangle** in the East makes it extremely vulnerable to such activities. India is having hostile neighbours and instable governments in the neighbouring countries due to which these activities flourish in the region. Also, **history** of extremism, insurgency, armed conflicts make it 'hot bed' for such illicit activities. The fallouts of **globalisation** has led to new opportunities and market for these groups. The globalisation of the economy has definitely helped the crime syndicates carry out their illegal activities across the borders with great ease. This has been further facilitated by the phenomenon of **'digital money'**. They very conveniently find safe havens outside the country. Unholy nexus between politicians, bureaucrats and criminals has led to the patronage to organised crimes and groups. **Criminalisation of politics** and **politicisation of criminals** is the major cause behind organised crimes as muscle and money power has become synonymous with political power.

4.2. ORGANISED CRIME: A MAJOR CAUSE FOR CONCERN

Organised crime (OC) is highly sophisticated and widespread illegal activity that drains billions of dollars from the global and national economy by illegal use of force, fraud, and corruption. These activities weaken the stability of the nation's economic system (as they evade taxes and legality) and affects all economic and social sectors and sections of society. It harms competing organisations, interferes with free competition, burdens interstate and foreign commerce and in turn threatens the safety, security and welfare of the nation and its citizens. Organised Crime has potential to rupture social cohesion, divide the institution of family, corrupt institutions and damage the democratic functioning of the country. Organised crime thrives in the areas where strict enforcement of law and order is not present or the authorities responsible for it, turn a blind eye. It acts as a catalyst for several other forms of violence, crime and internal security threats by providing financial and logistical support in the form of weapons to insurgents through arms smuggling. They use drug money to fund militants and extremists and give logistical support to terror networks too.

4.2.1. Challenges in Dealing with the Organised Crime

India does not have any **central agency** dealing with organised crimes specifically which gives rise to issues of coordination between different agencies of states and centre. There is **lack of specific and exclusive laws** to deal with organised crime. The charges and punishment are through various provisions of IPC and CrPC and other laws, which are very scattered. Also, these laws target individuals and not entire gangs. So, even if one or two members of such organizations are captured, the larger criminal network remains strong and functional. **Loopholes in Criminal justice system** means huge backlog or pendency of cases. The Indian Judiciary has 4.5 crore pending cases (as of 2021). The delayed justice and poor investigation by police gives opportunities to the criminals to exploit the systemic loopholes and escape from the clutches of law, as they get acquitted or cases pile up in courts without much progress. **Anonymity of leadership** in organised criminal groups give the organization multiple layers of protection from action by the state. The gangs are structured in such a hierarchical manner that the actual leader is never identified. The gang members at the lower rung (small fish) are usually caught but the big fish prevails outside the pale of law. As per the seventh schedule of the constitution of India, police and public order are subjects under state list. But many **states lack initiative and resources** to deal with the organised crime. The transnational nature of these activities and non-cooperation of regional and neighbouring countries due to their vested interests encourages and helps criminal organizations to thrive.

4.3. TERRORISM AND ORGANIZED CRIME

4.3.1. Differences between Organized Crime and Terrorism

Terrorism is sometimes considered to be another form of organized criminal behaviour, but the two are distinct from each other in important ways. Terrorism has a political objective. It involves crimes committed with the objective to intimidate a population or to compel government in conceding political objectives of the terrorists. For example, taking hostages for securing freedom of ideological compatriots. Organized crime, on the other hand, always seeks to obtain financial or other material benefits, with power and control being secondary motives. Terrorism is an act of political defiance that is carried out overtly, organized crime is mostly conducted covertly to earn profits. At the same time, terrorist acts are carried out to change the status quo whereas the organised crime gangs aim to run a parallel economy.

4.3.2. Linkages between Organised Crime and Terrorism

Though the objectives and operation methods underlying organised crime and terrorism are different from each other, sometimes differentiating the two could be difficult. Terrorist groups indulge in crimes traditionally linked with organised crime syndicates to generate revenue. This revenue is used to fund the activities related to their political or ideological agendas. For example, the chief source of revenue for Taliban has been **drug trafficking** and for ISIS, it has been trafficking of women, capturing oil wells illegally etc. Organized crime and its tactics of violence and coercion, **lack of concern for public safety** and inherent objective of social or national harm makes it useful for terrorists even when the terrorists and criminals are not directly cooperating for common ends. But it is seen that the organised **crime groups often act as subordinate organisations** to terrorist groups. They provide smuggled arms and explosives to terrorist gangs in exchange for drugs, diamonds, money, etc. Creating fake passports, smuggling terrorists into countries are among activities done by organised crime groups. Terrorists use networks established by transnational organised gangs to move men and material around the world. Many of the terrorist organisations transition between being terror organisations and organised crime groups, which helps them sustain through periods of inactivity and get back to life when the situation is appropriate. Thus, there is a **continuum** between the seemingly economic ends of criminal gangs and the political interests of terrorists.

There is an element of **mutual learning** and application of those on the **modus operandi** between organized criminals and terrorists. Organised criminals adopt the techniques used by terrorist organisations to achieve economic gains through manipulation and intimidation of public. They take advantage of existing corruption and unholy nexus between politicians, bureaucracy and criminals gangs. In similar veins, terrorists have been adopting the methods devised by organized crime networks for their ends. The second half of 1990s witnessed a number of terrorist groups learning from and through organised crime networks, like how to enter and escape for any country's jurisdiction undetected. They adopted methods and unique ways of smuggling such as through fake family, underground tunnels near borders. After 9/11, the United Nations Security Council (UNSC) adopted a resolution that recognized the **close connection** between global terrorism and transnational organized crime. The mutual dependence is starkly visible in drug smuggling along the **Golden Crescent and Golden Triangle on west and east of India** respectively. Both regions see anarchist groups, rebel armies and terrorists thriving on back of illegal trade in narcotics. The recent takeover of Afghanistan by **Taliban** has fuelled fears of growth of drug syndicates in the region. For example, in November 2021, 3 tonnes of Heroine was seized from Mundra port in Gujarat from a container coming from Kandahar, and headed to Andhra Pradesh.

Human trafficking is an associated trade of these drug networks. Young men with backpacks containing heroine cross borders moving drugs across Pakistan, Iran, Turkey, and beyond with help of established underground networks. The traffickers also use violence, fake promises of education and job, fraudulent employment agencies to trick and coerce their victims. The trafficked people often receive only the bare minimum compensation to live (food, water, shelter) while the money earned by their work in drug logistics goes to the traffickers. Narcotics trafficking and its collateral violence depend heavily on the availability of small arms. Thus, gunrunning is an associated industry. The Afghanistan–Pakistan region arguably has the world's largest concentration of illicit weapons, a situation made more volatile by the region's centrality in terrorist and extremist ideology. Similarly, in the east, for a long time, madrassas and mosques sponsored by the ISI in the Sylhet and Cox Bazaar areas of Bangladesh were being used to hoard and transfer arms procured by the ULFA from Thailand and Myanmar. ISI enabled ULFA to buy arms in Cambodia and pay for them in currency smuggled through Nepal. The militant organizations in India's north-east continue to source their weapons from the gunrunning industry of the golden triangle.

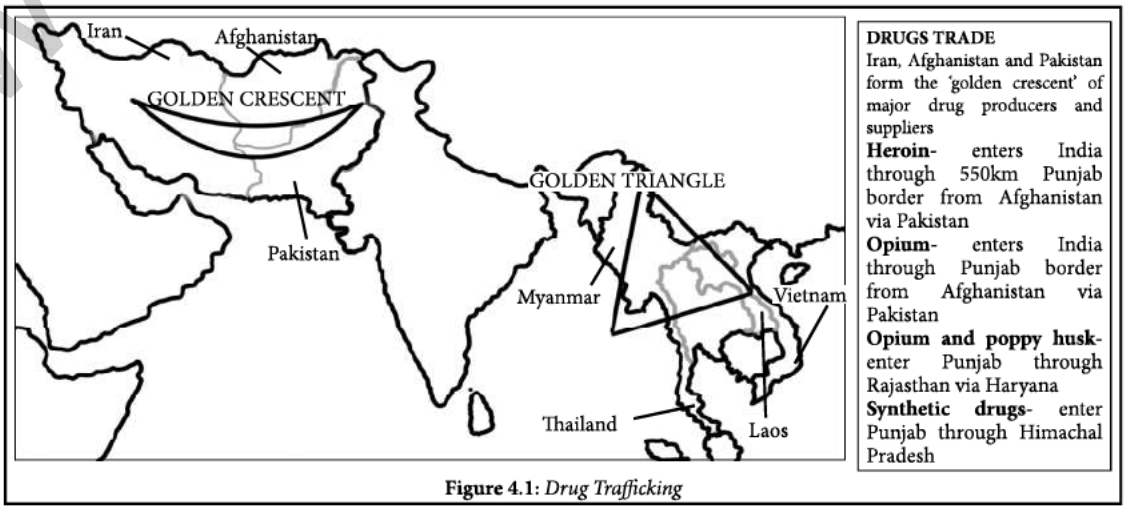


Figure 4.1: *Drug Trafficking*

Q. India's proximity to two of the world's biggest illicit opium-growing states has enhanced her internal security concerns. Explain the linkages between drug trafficking and other illicit activities such as gunrunning, money laundering and human trafficking. What countermeasures should be taken to prevent the same?
(UPSC 2019)

4.4. ORGANISED CRIME AND TERRORISM: INDIAN CASE

In India, the linkages between the terrorists and organised crime exist at national and transnational levels. In the **northeast**, the insurgents run parallel governments and control remote areas, out of bounds of the government. They collect money as tax from the people and at times from the government officials too. The Government officials are either bribed or threatened to award contracts in favour of the insurgents. The insurgents mobilise funds by smuggling drugs, arms and human beings across borders. Moreh, Chittagong Hill tracts, Cox's Bazaar act as some of the transit points for smuggling. In **Jammu and Kashmir**, the linkages between organised criminal gangs and terrorists are very different. They do not run parallel governments, nor do drug trade or extortion for funds. Their sources of funds are external and mainly arising out of Pakistan and PoK. Money laundering is the chief means of channelling funds. The hand of ISI, the intelligence service of Pakistan is suspected to be a major source of funding for militant activities in Kashmir. NIA has been actively unravelling terror funding activities in name of Zakat by Jamaat-e-Islami and its members in Jammu and Kashmir. In **other parts of India**, cities like Mumbai witnessed close links between terrorists and organised crime syndicates. The serial bomb blasts of 1993 in Bombay exposed the connection between terrorism and organised gangs.

4.5. BREAKING THE LINKAGES BETWEEN ORGANIZED CRIME AND TERRORISM

Given the mutually reinforcing nature of support provided by organized crimes to terror operations, it is imperative that this linkage between the criminal networks and terror modules be broken off. To achieve this objective, a multi-pronged strategy would be needed, whose components could include the following:

4.5.1. Strengthening International Co-operation

The globalised nature of organised crime requires a concerted cooperation and effort of several nations. Advanced and fast means of transport and communication enable the criminals to flee one country to another within hours of committing the crime. Through the internet revolution, criminal gangs control activities spanning continents without any physical presence. The recruitment of Indian youths by ISIS sympathisers was possible through Internet. The fugitives escaping to other countries cannot be punished or brought back for justice. Efforts should include to track and control hawala transactions, money laundering etc. International co-operation should be based on factors like a) swift **extradition** of criminals, b) agreement on mutual assistance in various subjects from foreign countries, c) Stemming cross-border flow of material and ideological support for organized crimes and terrorism targeting neighbouring countries d) multi-lateral mechanisms for **transfer of data** on crimes and mutual sharing of knowledge e) Tracking and stopping the flow of finances, especially in name of development assistance and aid, to individuals, groups, and countries perpetuating terrorism. The role of **FATF** is important in the context of need for global co-operation in breaking the linkages of terrorism with organised crimes and stopping money laundering, along with taking coercive financial action against non-cooperative regimes.

4.5.2. Reforming Political System and Bringing in New Laws

The **Vohra Committee Report** exposed the relationship between politicians and criminal gangs. Politicians depend on criminal gangs for funding their elections and muscle power to rig elections or capture booth. To bring this nexus to

an end, election reforms are necessary and for that to take place strong commitment on behalf of the political parties is required. Now, Criminals have easily gained access to politics based on money and muscle power. The **Second ARC** has highlighted that India needs to enact a comprehensive central law which will deal with all organised crimes comprehensively. Specific provisions to define organised crimes should be included in the new law governing **'Federal Crimes'**. The definition of organised crime in this law should be on the lines of the Maharashtra Control of Organised Crime Act, 1999.

4.5.3. Strengthening Law Enforcement Agencies

A strong police force is an anathema of criminal gangs. Aftermath of 1993 Mumbai blasts Mumbai Police got immense success and was accoladed for putting an end to activities of criminal gangs in Mumbai. A highly professional, motivated and ethical police force can prevent the emergence of any criminal gang. They have eyes and ears on the ground which can be developed as informal intelligence sources. Cooperation between different intelligence agencies, law enforcement authorities and innovative solutions are needed to thwart the ulterior motives of criminal gangs and their possible nexus with terrorists. Rehabilitation of Chambal dacoits and gangs through initiatives which included pension for those leaving dacoit work was a successful model for thwarting growth of illicit activities.

4.5.4. Role of Media and Society

Mass media, both print and electronic can play an important role in exposing organised crime and help build public opinion against it. Investigative journalism helps to expose the activities of criminal gangs. Social media is emerging as a tool for organized gangs and terrorists in co-ordinating their operations and logistics, but social media can also play a major role in mobilising public opinion and awareness against organized crimes and criminal gangs. Civil Society can also play an important role to break the chain of making politicians having criminal backgrounds as legislators.

Organised crime has toxic tentacles that are not only directly harmful to society through the illegal operations and violence but such groups act as conduits of terror operations. Addressing the problem of terrorism and curbing its use by **state and non-state actors** for political and social intimidation requires putting effective curbs on organized crime. The linkage between terror and crime needs to be permanently ruptured across the world to cut through the roots and branches of terrorism. The interlinking and globally widespread supply, transit and demand networks of terror and organised crime require a stronger global response that appreciates the threat that terror and crime pose to **peace** in the world.

Q. Analyse the complexity and intensity of terrorism, its causes, linkages and obnoxious nexus. Also suggest measures required to be taken to eradicate the menace of terrorism. **(UPSC 2021)**

Militancy in Jammu and Kashmir

5.1. INTRODUCTION

The valley of Kashmir has been eulogized as a paradise on earth most famously by Jahangir, the Mughal emperor. The region is surrounded by tall mountains on all sides. People of Kashmir consider these mountains as their guardian and protector. Since ages, people of various religions and cultures have come into the valley and made it their permanent home. This can be witnessed in Kashmir becoming the home to Buddhists, the dwelling place for the Vedanta and a center for mystic Islam.

5.1.1. Historical Background

Kashmir's history has witnessed the rule of various dynasties. The ancient history can be traced in **Rajatarangini** which gives a formal account of Kashmir's history. After the period of Buddhist and Hindu kings, Kashmir was ruled in the medieval times by the **Sultans, Moguls, Afghans, Sikhs and Dogras**. Thus, Hinduism, Buddhism, and Islam together made a significant impact on the life of Kashmiris. The experience of coexistence turned Kashmir into a melting pot of multiple communities living in harmony for centuries. The people of Kashmir call the valley Pirwaer and Rishwaer, the abode of Sufis and Rishis.

In 1820, the Jammu and Kashmir became part of the **Sikh Empire** under Maharaja Ranjit Singh. Later the British empire fought a battle with Sikhs after the death of Maharaja Ranjit Singh, in which Gulab Singh (a Dogra general in Maharaja Ranjit Singh's army) sided with the British. When the Sikhs lost and the **Treaty of Amritsar** was signed in 1846, Kashmir was given to Gulab Singh as a reward and on condition of acceptance of British sovereignty. Since then, till independence of India in 1947, Kashmir was ruled by the Dogra dynasty. Hari Singh took charge of the state in 1925. He was the king of Kashmir when the treaty or Instrument of Accession was signed with India. You can read about the post-independence issue related to Kashmir accession in detail in the post-independence booklet.

Instrument of Accession was signed by Hari Singh on 27th Oct, 1947 and it led to accession of Jammu and Kashmir (J&K) into the Indian dominion. J&K was granted a special status under Article 370 of India's Constitution. However, the erstwhile princely state surrendered only three subjects-**defence, external affairs and communications** to the Indian government. Government of India agreed for a separate constituent assembly to formulate Jammu and Kashmir's separate constitution. **Article 370** explicitly mentioned that only the provisions of Article 1 and Article 370 applied to the state. But India included Article 370 in Part XXI of the Indian Constitution, under the heading '**Temporary, Transitional and Special Provisions'**. While the special status allowed J&K to have its own constitution and flag, it also maintained that the Government of India could extend the central laws on subjects included in the Instrument of Accession, viz., Defence, External Affairs and Communications — by 'consultation' with the state government. Moreover, the remaining central

laws could be extended to the state only with the 'concurrence' of the state government. This gave the legislative assembly of Jammu and Kashmir extraordinary powers.

The **special provisions for J&K under Article 370 and 35A** had been a contentious issue from the very time of accession of J&K to India. Various national leaders were apprehensive of the special status given to the state. **B R Ambedkar** had said that enacting such measures would be ***'treacherous thing against the interests of India'***. **SP Mukherjee** launched a Satyagraha campaign against special provisions for J&K under the slogan "*Ek desh mein do Vidhan, do Pradhan aur Do Nishan nahi chalenge*" (A single country cannot have two constitutions, two prime ministers, and two national symbols). On the other hand, there were political factions in Kashmir who wanted Kashmiri Muslims to secede from the secular Indian state and would express this sentiment through demand for right to self-determination or plebiscite. While such demands persisted, numerous Presidential Orders under article 370 were passed over the years, extending more and more provisions of the Constitution of India and the central legislations to J&K, which practically placed the state at par with other states. After the Indian victory in the 1971 Indo-Pak war and the **Indira-Sheikh Accord** of 1975, the demands for plebiscite and secession had been practically settled, till the rise of militancy in Kashmir during late 1980s.

5.2. REASONS BEHIND MILITANCY IN JAMMU AND KASHMIR

Major causes which have led to and still exacerbate Kashmir militancy are related to **role of Pakistan**, alleged **rigging of 1987 elections** to Jammu and Kashmir legislative assembly, and **religious radicalization.**

The first and foremost reason for Jammu and Kashmir militancy lies in Pakistan-sponsored terrorism in the region. The role of Pakistan has also been acknowledged by the Federal Bureau of Investigation (FBI) in 2011 in US Court, where it said that the Inter-Services Intelligence (ISI) sponsored terrorism and separatist groups in Kashmir. After the **retreat of the Soviet Union from Afghanistan** in 1988-89, Mujahideen -fighters raised against the Soviets were diverted to Kashmir. Pakistan helped them infiltrate Kashmir with the goal of spreading radical Islamist ideology. Moreover, during 1987 election, various radicalized anti-establishment Islamic groups including Jamaat-e-Islami Kashmir organized themselves under a single banner named Muslim United Front (MUF). MUF's election manifesto included working for Islamic unity, implementing the law of Quran or Shariat and resisting any kind of political interference from the center. But it won only 4 seats even with 31% of votes polled. The supporters of these parties alleged that elections were rigged and this led to rise of insurgency in the valley at catastrophic level.

Over the years, the declining **credibility of political parties** and ineffective administrative machinery has contributed to the growing disenchantment among the youth. The disruption in the academics, frequent strikes, the law & order situation, students' agitation disrupts the hopes for a better future. Incidents of high handedness of security personnel to control the situation on the ground including the use of pellet guns etc. aggravates conflicts with local people, widening the trust deficit between people and the Indian state. The lack of affinity for the state among the people is exploited by terrorist organizations and separatists. In addition, issues of high **unemployment and lack of economic opportunities** have created incentives to youth to be attracted towards militancy. While the youth remained consumed in militancy, the situation of unrest and threats of terrorism have harmed the tourism potential of Kashmir despite its scenic beauty. This situation further hinders the economic prospects of J&K and create a vicious cycle of unrest and dissatisfaction among the people. These issues are often misused and misrepresented by separatist leaders, putting the blame on the central and state government and projecting the demand for a separate nation as the only way forward.

The 'Human-shield' Incident

In 2017, Farooq Dar, a local Kashmiri, was tied to the bonnet of an Army Jeep by Major Leetul Gogoi of the Indian Army in a bid to handle a volatile situation of impending stone-pelting. The image of Dar being used as a 'human-shield' made international headlines and put in spotlights the civilian-military conflict in Kashmir. In interviews to media, a year after the incident, Dar revealed that he was boycotted by villagers who considered him a government agent. He claims to suffer from insomnia and depression due to the incident.

Apart from above reasons, **religious radicalization** is among the primary causes for the rise of militancy in Kashmir. Radicalization happens through a mix of factors like when the people are already agitated, are deprived of resources, are subjected to influence and **intimidation of militancy** in their neighborhood and are fed up with communal propaganda. Radicalization inspires people to fight against those who belong to a religion different from theirs and it convinces them to consider the interest of communities as antagonistic. Idealization of terrorists like Burhan Wani and **romanticization of 'gun culture'** through social media posts is a major cause for rise in number of local militants. Youth in Kashmir often grow up in an environment of conflict seeing guns, arms, ammunitions as a symbol of might. Many of them get fascinated by the thrill and glamour of gun culture and are lured by the commando-styled attires of the militants and weapons. Social condoning of acts of terrorism through large gatherings in funeral processions of terrorists creates lasting impressions on young minds. This deepens the problem of militancy among youth.

Social media and mainstream media are also playing a major role in radicalization of youth. Messages on WhatsApp groups are forwarded with aim to mobilize people for stone-pelting, protests etc. Instagram posts of militants, fiery speeches of terrorists are widely circulated. Pictures posted on social media attract the lay youngsters as it gives them promise of instant fame, recognition and respect in an environment where there are hardly any other platforms for their aspirations. This misguided inspiration and disenchantment of youth results in an increasing number of youths adopting the path of militancy in their school and college days. Further, experts have highlighted that sensationist coverage of Kashmir issue in **mainstream Indian media** acts as a barrier in integration of Kashmiri youth into the national mainstream. Often, it has been alleged by Kashmiri people that mainstream media portrays all Kashmiris as terrorists. In addition, round-the-clock bitter debates on communal matters involving fanatic religious leaders create a highly polarized environment. Hindu-Muslim dynamics in India has an enormous impact on the mindset of Kashmiri people such as the incidents of beef-lynching and communal riots.

The role of **Pakistani propaganda** is also an important factor in keeping militancy alive in Kashmir. The goal of such propaganda is to present the legitimacy of Indian rule in Kashmir as disputed, create international pressure on India to negotiate with Pakistan while providing continuous **cover and encouragement to insurgency.** International condemnation of India's handling of Kashmir issue is also sought to hinder anti-militancy actions of Indian security forces on the ground through criticism of India in various human rights organizations. In addition to existing challenges,China Pakistan Economic Corridor (CPEC) presents itself as a significant challenge to the internal security of the region. CPEC, a cardinal subset of OBOR (One Belt One Road), presents itself as a significant threat to internal security of not only Jammu and Kashmir but entire nation. The CPEC is bilateral project between Pakistan and China. Its stated objective is to enhance connectivity across Pakistan with a network of highways, railways, and pipelines accompanied by other infrastructure development projects. Under CPEC plan, China is investing in industrial

power stations, roads and railways from Kashgar in Xinjiang (China) to Gwadar port (Pakistan) in the 3000 km long belt.

India has preferred to distance itself from CPEC initiative for various reasons associated with geo-politics, security, stability and most importantly sovereignty. The proposed China Pakistan Economic Corridor (CPEC) passes through the Pakistan occupied Kashmir (PoK) and thus violates India's sovereignty. In addition, if the CPEC project reaches its end it will lead to encircling of India by China from both Eastern (LAC) and western side (CPEC). Further, even though China/Pakistan claim that it is an infrastructure project, in reality it is so designed that its strategic components can-not be overlooked. Moreover, CPEC will end China's Malacca dilemma and can also disrupt the SLOC (Sea Lines of Communication). Also, CPEC will have the effect of making Pakistan a proxy in the hands of China, as the two are set to start as partners but it is inevitable that eventually Pakistan falls into the debt trap of China. Lastly, CPEC may help China in emerging as a 'direct party' in the Kashmir dispute in future.

Q1. The China Pakistan Economic Corridor (CPEC) is viewed as a cardinal subset of China's larger 'One Belt One Road' initiative. Give a brief description of CPEC and enumerate the reasons why India has distanced itself from the same. **(UPSC 2018)**

Q2. China and Pakistan have entered into an agreement for development of an economic corridor. What threat does this pose for India's security? Critically examine. **(UPSC 2014)**

5.3. IMPACT OF MILITANCY

The most important issue arising out of continued militancy in Kashmir is the threat it poses to foundational principles of the constitutional and civilizational identity of India. The **exodus of Kashmiri pandits** from the valley since the early 1990s is directly attributed to rise of militancy in Kashmir along with the social support for it which reflected a rising tide of religious radicalization. The resultant spurt in violence, communal threats and targeted killings in the valley forced Kashmiri Pandits to move out of their homes and in one big sweep destroyed the millennia-old religious pluralism of the valley. The community of Kashmiri Pandits have since been forced to live in migrant colonies lacking basic amenities. Many efforts have been made for their return to Kashmir but assurance of security to their life and property, livelihood opportunities still remain a challenge. The question of their homecoming is also a political and emotional issue which is subject to communalization adding to the layers of complexities in the issue of Kashmir.

Militancy in Kashmir poses **threat to the national security,** integrity and sovereignty of the country. At various occasions we have witnessed bomb blasts and attacks in different parts of the country originating from Kashmir with the support of Pakistan. **Parliament attack in 2001** was also planned and executed by such militants. Sovereignty concerns are affected when terrorists and separatist groups vouch for Pakistan's interests and demand separation from India. The Kashmir militancy also raises concerns related to the safety of people living along the border with Pakistan as well as in deep hinterlands and cities. Shelling by Pakistani army to support infiltration of terrorists causes death, injury and loss of property for villagers living along the borders, including the damage to schools etc. Increased presence of **Indian security forces in the valley,** encounters between security forces and terrorist groups at times affects the day-to-day life of the common man. Deaths of civilians and loss of property are often considered as collateral damage in handling and safeguarding security interests.

Regular inspections, combat operations with terrorists, violence, deaths create an atmosphere of uncertainty in the minds of people. The situation gets compounded by attacks on officials, vital governmental buildings and other infrastructure in the state. This leads to **disruption in governance** and further weakening of developmental prospects of the region. Impact on governance leads to a reduction in the belief and **trust of the people in democratic values** and institutions. These issues do not remain localized only at the individual level but also have wide ranging social repercussions. Continuous war leads to **development of a feeling of alienation** from the rest of the country. Such

feelings are exploited by terrorists, separatist groups and Pakistan to propagate anti-India sentiments among people of Kashmir using propaganda. The rise in propaganda also leads to increased radicalization specially among youth who adopt extreme political, social, or religious ideals and aspirations, undermining the native culture of inclusive coexistence.

The situation of militancy in Jammu and Kashmir also has considerable economic impact. The continued situation of conflicts makes industries apprehensive of establishing themselves in this region, restraining investments, infrastructure and any new project in the region. Militancy, thus, directly creates issues of lack of job creation and economic opportunities for the locals. Further, the scope that tourism offers to this place is also severely constrained. In this scenario, there is considerable **revenue loss to the exchequer** and **opportunity loss for the people.**

Movies in Kashmir

Bollywood's love for the picturesque Kashmir dates back to the decades of 60s when a number of movies were set in the backdrop of the beautiful mountains of the Valley. The most romantic and evergreen songs were picturized in the snow-clad hills and lush green slopes of Jammu & Kashmir. Shammi Kapoor immortalized the 'shikara' on the Dal Lake in the song *"tareef karun kya uski"* as he wooed the beautiful Sharmila Tagore in Kashmir Ki Kali (1964). In the late 1970s and early 80s, cinephiles witnessed the beauty of the valley in superhits like Kabhi Kabhi (1976) and Silsila (1981). For those growing up in urban India, visiting the 'paradise on earth' became a dream. Thus, the movies which captured nature in Jammu and Kashmir its full glory also gave a major fillip to the tourism sector. People who could not visit the scenic meadows of Sonmarg or the Tulips in Srinagar enjoyed their serenity and captivating beauty through the lens of filmmakers.

Kashmir Ki Kali (1964) at Dal Lake

Silsila (1981) at an Apple orchard in Kashmir

By the 1990s, the region witnessed some of the most violent times. The rising unrest forced filmmakers to look for alternate locations. Maniratnam wanted to shoot his classic Roja (1992) in Kashmir, but ended up shifting it to Ooty and Manali. Other directors chose foreign locales. Over time, a sense of fear and uncertainty engulfed Bollywood's once favorite backdrop and Swiss mountains replaced the Peer Panjal in Bollywood classics of the 90s.

Darr (1993) in Swiss Alps

Jab Tak Hai Jaan (2012) in Dal Lake

However, in recent times movies or parts of them have started to be shot in the valley again as the violence seemed to subside in comparison to nadir of the 1990s. Some major Bollywood productions shot recently in Kashmir include Jab Tak Hai Jaan (2012), Haidar (2014), Bajrangi Bhaijan (2015), Raazi (2018) etc.

5.4. CHALLENGES IN DEALING WITH MILITANCY

Many efforts have been taken by the Government of India to bring peace in the region and deal with Kashmir militancy. However, the problem of militancy has persisted due to various factors.

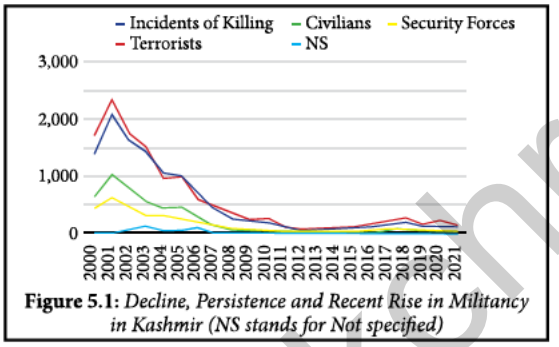


Figure 5.1: *Decline, Persistence and Recent Rise in Militancy in Kashmir (NS stands for Not specified)*

One such important factor is the **role of Pakistan** in supplying weapons, militants and radical ideology across the border. Pakistan aims at keeping the population on the boil, inciting people to agitate against India and abetting young people towards stone-pelting, espionage, or to work as overground support for terrorism, apart from direct involvement in terrorist acts. A major problem is the rise in number of **local militants** in Kashmiri militancy, which was earlier fueled by mainly the foreign fighters recruited from terror outfits in Pakistan. Due to involvement of locals, the militancy continues even when the external support from across the border is cut-off. Moreover, it becomes difficult to target local militants as they are our own people and strong actions against them gives rise to an emotional support for their actions among many Kashmiri people. The involvement of **overground support** for militants has also become complex as militant groups label acts like stone-pelting by mobs as jihad. This tactic is used to keep up local support, getting more recruits and involving youth in activities against the security forces, even if they cannot join a militant outfit due to various reasons.

Year	Recruitment of militants by terrorist organizations in J&K
2010	52
2011	23
2012	21
2013	16
2014	53
2015	66
2016	88
2017	128
2018	218

In present days, the challenges in handling militancy becomes all the more difficult when youth with no predictable and certain future are trying to emulate the ideals of terrorists, considering them as heroes and celebrating their deaths and anniversaries. The menace of internet-based propaganda and misinformation from Pakistan is difficult to eliminate due to lack of territorial jurisdiction. Vast amount of effort and machinery is being used to reintegrate misdirected and radicalized youth back into the mainstream. But, as can be seen from above discussion, handling local militancy and cutting off their external and internal **financial, social and ideological support** remains a major challenge for both the governmental organizations and security forces.

A big challenge is building a better **perception among Kashmiris** about the Indian state, its constitutional ethos and pluralistic identity. It is seen that although the resources allocated directly or indirectly to J&K has been increasing manifold on account of provisions for security, infrastructure and employment opportunities to the people, it has still not brought a total shift in the minds of Kashmiri people in favor of the Indian government. The problems in Kashmir are not an economical or security challenge alone but have deep roots in issues related to trust and belief in the constitutional

framework of India. **Poor employment options** due a deficit of economic avenues and industries in the state also aggravate the discontent of people. According to a report of the Hindu, J&K received ₹1.14 lakh crore (10 percent) of all Central grants given to states over the 17-year period of 2000-2016, despite having only one percent of the country's population. However, due to misuse of central grants by J&K administration due to financial irregularities and widespread corruption, no substantive change has taken place in the lives and infrastructure in Kashmir. The poor economic development in Kashmir was also perpetuated by the presence of Article 370 because of which industrialists and entrepreneur from outside the state faced hindrances in getting land and permits to set up a business which retarded the growth of the state to a major extent. **Lack of stable government** has contributed in its own ways in continuance of militancy in J&K. Governments in J&K have often been of short-tenure. In past, accusations have surfaced with respect to legitimacy of free and fair conduct of elections. For example, the infamous 1987 legislative assembly elections are widely considered to having been rigged in favor of one party. Elections at local level are often not held within time leaving grassroot democracy in dysfunctional state. Such a state of affairs dissuades people from participating in the political process. The unaddressed aspirations are then fulfilled through terrorists and separatist groups in absence of a credible democratic process.

Various new challenges have also been seen to be emerging due to the revocation of Article 370. In wake of new developments related to article 370, the state has been kept under complete surveillance, multiple phases of internet shutdowns and larger deployment of security forces. This has led to **undermining of civil rights** of people living in Kashmir. Further, many experts have criticized the revocation of 370 as a move against federalism, arguing that it would further increase **alienation of Kashmiri people** from the rest of the country. Many leaders have argued the change as being against various Supreme Court judgements and a case of betrayal of trust of Kashmiri people. Some constitutional experts have also considered it as a case of colorable legislation in which a law is so made that it is able to do act indirectly on a matter which was not under its direct legislative competence. As a local political response to revocation of article 370, many political parties of J&K have come together to create the **People's Alliance for Gupkar Declaration (PAGD).** Apart from various political parties of J&K, the alliance also includes some national parties such as CPI(M). The alliance is aimed at restoring the special status of J&K including article 370 and article 35A, protecting against unconstitutional delimitation revoking the state's bifurcation. There have been concerns related to **the new domicile policy** of J&K. People from Kashmir think that the policy may endanger their cultural identity and entry of outsiders may lead to demographic change in the valley. Of late, it has been seen that the militants are targeting Hindu and Sikh civilians and migrant workers from Bihar and Uttar Pradesh. Creation of terrorist outfits such as **The Resistance Front (TRF)** on this issue is a concerning development. This and similar terror organizations are being created by the Pakistan army and the Inter-Services Intelligence (ISI) as a response to India's abrogation of Article 370. Indian agencies claim that the outfit is nothing but an offshoot of Lashkar-e-Taiba.

Alienation of locals and their disillusionment with political process has created a **cadre of overground workers (OGWs).** OGWs are people who provide logistic and other support to militant groups. They act as **eyes and ears of the terrorist organisations,** thus, providing them any outside information crucial for their plan and upcoming attacks. They convey details relating to either administration or security issues that can be exploited by terrorist organizations. They play a key role in tracking movements of all security forces in the region so as to aid the operations of these militant groups as well as in providing cover to them for escaping such as by arousing and mobilizing people for stone-pelting. The OWGs provide the background work for checking place of hideouts for the groups and make sure all the facilities are provided where the terrorists can make their plan of action. This keeps the terrorist groups on safe haven. Their timing of crossing borders, planting an attack, etc. is managed by the OGWs.

Q. The banning of 'Jammat-e-Islami' in Jammu and Kashmir brought into focus the role of over-ground workers (OGWs) in assisting terrorist organizations. Examine the role played by OGWs in assisting terrorist organizations in insurgency affected areas. Discuss measures to neutralize influence of OGWs. **(UPSC 2019)**

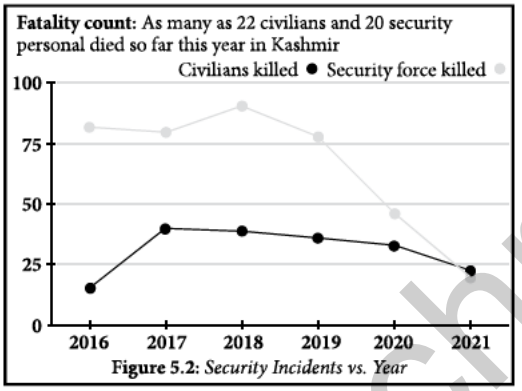


Figure 5.2: *Security Incidents vs. Year*

Apart from these challenges, there is an **emerging international challenge** due to the successful capture of power by Taliban in Afghanistan. It is being argued that the restoration of Taliban rule in Afghanistan will create issues for India's security. It may lead to Pakistan redirecting its jihadi groups who fought with Taliban towards J&K to launch new terror attacks and induce radicalization among the youth of Kashmir. The rise in Islamist sentiments under inspiration from Taliban is possible, which would pose threat to democracy. Kashmir's susceptibility to such ideological influence could be seen during rise of ISIS in West Asia as individuals would claim allegiance to ISIS, waving its characteristic flags during protests. Further, development of new geo-political alignments such as a **China-Pakistan-Taliban axis** may directly challenge India's interests in establishing peace in J&K. The renewed tensions along the Line of Actual Control in Ladakh between India and China in parallel to revocation of article 370 is a case in point.

5.5. RECENT STEPS TAKEN BY THE GOVERNMENT

Till their revocation, **Article 370 and Article 35A** were the enabling articles in the Indian constitution which restricted Indian citizens from other states to purchase land or property in Jammu & Kashmir and were aimed at protecting the rights of the natives. The special provisions ensured that residents of J&K had a separate set of laws related to citizenship, ownership of property and fundamental rights. However, it has been seen that these provisions acted as a deterrent for investment in the region and was **not able to satisfy the demands either of the Kashmiris or of the country as a whole.**

With the motive of J&K's complete constitutional integration into India, article 370 which gave special place to J&K in the constitution of India has been done away with on 5th August 2019. Also, the earlier state of Jammu and Kashmir with regions of Jammu, Kashmir and Ladakh has been reorganized into two union territories (UT) of J&K and Ladakh as per the Jammu and Kashmir Reorganization Act 2019. As per the provisions of the Act, the **new UT of Jammu and Kashmir will have a legislature** and Ladakh UT will be without a legislature. Both the UTs are now being administered through a Lieutenant Governor (LG) appointed by the President.

Separate constitution of J&K ceased to be in operation, thus ending its special powers like separate citizenship. Now the education, employment opportunities, land and property rights in the state will be open to not only all Indians, but to all sections of society within the state such as rights for minorities, tribals, scheduled and backward castes and women. The **Ranbir Penal Code** of the state is now replaced with **Indian Penal Code** with expanded provisions for **dowry deaths**, criminalization of **sexual intercourse with a girl aged 15-18,** decriminalization of **homosexuality** etc. that have come into effect due to **judicial** pronouncements on related sections of IPC. Duration of the **legislative assembly** of J&K which had been 6 years will now be **5 years.** All **constitutional provisions and laws** made by the parliament will be applicable to the LG. There will be a **common High Court** (the High Court of Jammu and Kashmir) for the Union Territories of Jammu and Kashmir as well as Ladakh. An Advocate General will provide legal advice to the

government of the Union Territory of Jammu and Kashmir. These reforms are aimed at bringing national integration, end discrimination (articles such as 35A), ensure economic growth and investment, tackle militancy, control corruption and prevent politicization of security issues in J&K and Ladakh, which are sensitive border regions.

Rashtriya Rifles: The Rashtriya Rifles is a counter insurgency force under the authority of the Ministry of Defence. The soldiers in the RR are deputed from other units of the Indian Army. The RR is currently deployed in the union territory of Jammu and Kashmir, as well as the Ladakh UT. All RR regiments are given specific and uniform training in counter-insurgency operations. RR regiments operate in the grid system, by physically dominating the insurgency affected areas. The RR have played a stellar role in conducting counter Insurgency operations in Jammu and Kashmir.

5.6. OTHER GOVERNMENT MEASURES AND SCHEMES

Government has time and again taken measures to address the various factors which fuel militancy in Kashmir. Schemes such as **PARVAAZ** aim to provide increased economic opportunities to youth. This scheme is for providing support to air cargo shipment of perishable products of agriculture and horticulture which are harvested in Jammu & Kashmir. A subsidy will be provided on the air cargo charges inclusive of the airport handling charges for shipments through empaneled airlines. This scheme aims at doubling the income of fruit growers and farmers of Jammu & Kashmir thereby ensuring their welfare. This scheme could also be adopted by the Animal, Sheep Husbandry and Fisheries departments for milk, fish and other perishables as per the available funds. **Himayat** is a placement-linked skill training programme for unemployed youth of Jammu and Kashmir and has been under implementation in the state since 2011. Under the programme, the youth are provided free skill training for a duration of 3 to 12 months, in a range of skills for which there is good market demand. At the end of the training, the youth are assured of a job and there is one-year post-placement tracking to see how they are performing. The Programme is 100% funded by the Government of India. It covers both urban and rural populations irrespective of levels of poverty.

Udaan scheme is a Special Industry Initiative for Jammu & Kashmir. It is in the nature of the partnership between the corporates of India and Ministry of Home Affairs and implemented by National Skill Development Corporation (NSDC). It aims to provide skill training and enhance the employability of unemployed youth of J&K. It covers graduates, postgraduates and three-year engineering diploma holders. Its objective lies in providing an exposure to the unemployed graduates to the best of Corporate India and providing corporate exposure to the rich talent pool available in the State. Earlier, central schemes in Jammu and Kashmir faced various implementation challenges. This has been done away with by abrogating the special status and **extending all the central schemes to Union territory** of J&K. These people-oriented development schemes included PM-KISAN, PM-KISAN-Pension, Pradhan Mantri Jan Dhan Yojana and Stand-Up India etc. Schemes like **'Nai Manzil'** and **'USTAAD'** aim at exploiting the full potential of individuals from minority communities, thus providing support to youth from Kashmir who are predominantly Muslims. Nai Manzil Scheme is an integrated Education and Livelihood Initiative for the Minority Communities aiming to benefit the minority school drop-outs youths in the community education institutions like Madrasas. It will provide them an integral input of formal education (up till Class VIII or X) and skill training along with certification. **USTAAD** (Upgrading the Skills and Training in Traditional Arts/Crafts for Development) scheme on the other hand aims to preserve the rich heritage of traditional arts and crafts of minorities and build capacity of traditional artisans and craftsmen.

To deal with the **alienation of locals with the security personnels**, efforts have been taken for **confidence building** and reducing mutual mistrust. The security forces are under instructions to respect the human rights of all people and work steadfastly with a humane face while performing

their day-to-day operational duties. Moreover, every reported case of alleged human rights violations is taken seriously and the investigation is done in a transparent manner. This ensures that the human rights of locals remain protected and intact. Establishment of **youth clubs at Panchayat level** is targeting increased engagement of youth in the political process and to facilitate their integration into the mainstream. At times, various individuals who are lured into militancy face a **crisis of conscience** and want to return back. To encourage such incidents of change of heart, **surrender and rehabilitation policy** has been offered. The objective of the policy is to encourage people to adopt peaceful methods and accept the integrity of India and abide by the Indian Constitution. The policy thus facilitates the return of ex-militants who belong to J&K state and had crossed over the PoK/ Pakistan for training in insurgency but have given up insurgent activities due to a change of heart and are willing to return to the State. It encourages them to join the mainstream and lead a normal life and contribute towards prosperity and progress of the State as well as the nation.

5.7. INTERNATIONAL AND BILATERAL MEASURES FOR PEACE

India has also taken up various measures at bilateral and international level. After the partition of India, when a dispute erupted between the two States, India took this matter to the UNSC. It passed resolution 39 (1948) and established the **United Nations Commission for India and Pakistan** (UNCIP) to investigate the issues and mediate between the two countries. Further it also established the **United Nations Military Observer Group for India and Pakistan (UNMOGIP)** by resolution 47 (1948) to monitor the cease-fire line. But over years, the international influence including of UNSC resolutions proved to be unfruitful and subject to big power politics of the times. As a result, India continues to emphasize bilateral discussions over international interventions or mediation for achieving peaceful resolution of the issue. For example, under the **Shimla Agreement (1972)**, India and Pakistan agreed to settle their differences by peaceful means through bilateral negotiations.

The bilateral methods for peace have included **confidence-building measures** (CBMs) like bus services and trade across the Line of Control. India and Pakistan started *Karavan-e-Aman* (*Caravan of Peace*), a bus service connecting Srinagar (Jammu & Kashmir) and Muzaffarabad (Pak-Occupied Kashmir) in 2005. In 2006, a second bus service started between Poonch (Jammu and Kashmir) and Rawalakot (Pak-occupied Kashmir). In 2008, trade was started on these routes, opening Jammu and Kashmir's traditional trading centers to the west for the first time since 1947. The trade is tightly regulated. During times of heightened tensions between India and Pakistan, these routes are closed, as was the case in 2019 as an aftermath of Pulwama terrorist attack or in 2020 in wake of revocation of article 370.

Various mechanisms for bilateral dialogue between governments of India and Pakistan have been launched over the years. **Conventional mechanisms** for dialogue include the 1998 composite dialogue process which for the first-time mentioned reference to all outstanding issues including Jammu and Kashmir, followed by 1999 Lahore visit of PM Atal Bihari Vajpayee and **Lahore Declaration** which suffered a setback by the Kargil war. 2001 Agra Summit failed due to intransigence of Pakistan on Kashmir issue. 2004-05 saw resumption of composite dialogue. The 26/11 attacks in 2008 disrupted the bilateral dialogues again. The resumed dialogue in 2010 included counter-terrorism and Mumbai attack trials. Border incident of beheading of India soldier at Line of Control stalled dialogue in 2012. **2015 Ufa declaration** saw resumption of dialogue between Indian and Pakistan after backchannel talks through **track-II diplomatic mechanisms**. 2015 also saw Indian Prime Minister Narendra Modi visiting Pakistan in an officially unscheduled stop-over during his flight from Kabul to Delhi. A spate of terror attacks over next few years disrupted the bilateral dialogues again.

Track-II diplomacy is the practice of non-governmental, informal and unofficial contacts and activities between private citizens or groups. It contrasts with track I diplomacy, which is the conventional diplomacy by governments held through official government channels. However, track-II diplomacy is not a substitute for track one diplomacy. Track-II is supposed to assist officials in managing conflicts by exploring possible solutions away from the public view and without the requirements of formal negotiations. In addition, the term **track 1.5 diplomacy** is used by some analysts for situations of official and non-official actors cooperating in conflict resolution. In India, the **'Neemrana dialogue'** was launched in 1991 as a track-II initiative between India and Pakistan, which has continued intermittently amidst disruption due to terror attacks such as 26/11 attacks in Mumbai or Uri attacks. The latest round of track-2 dialogue took place in in April 2018. Topics discussed in the dialogue included Kashmir, Siachen conflict and the situation at the Line of Control.

In recent times, India has also garnered support from other countries such as Russia which has backed India's move to change the provisions of Article 370 and has stated that the reorganization of J&K is an internal matter of India. Several other countries like the USA, UAE etc. have called it an internal matter of India which reflected diplomatic success in forging stronger ties with countries from the Gulf to across the Indo-pacific and international isolation of Pakistan on the issue of terrorism and decreasing sympathies for its position on Kashmir

5.8. WAY AHEAD

Due to a host of measures adopted to achieve peace in the region, certain positive outcomes have been achieved. These include success against smuggling of weapons, control over infiltration across the line of control, deterrence against major terrorist attacks due to assured and strong counter-response, action against over-ground supporters, humanist approach to conflict handling and development. As a result, perpetrators of violence are finding it increasingly difficult to send weapons and militants across the border due to increased vigilance and border fencing. Further, Pakistan at present faces global condemnation as a terror-sponsoring country and is placed under grey list of Financial Action Task Force (FATF). The global mandate is against terrorism as almost every country have suffered due to it in the past.

However, challenges such as of technology as seen in drone attack at Jammu Air Force Station, geo-political implications of Taliban's ascend to power in Afghanistan, or the China-Pakistan axis and problems of infiltration and incursions continue to pose serious harm to peace in Jammu and Kashmir while threatening India's security and territorial integrity. The way ahead is to adopt **multidimensional measures** which can deal with the various aspects of militancy in J&K and address needs of regional security

The first focus should be on handling the existing imminent security threats that the militancy of Jammu and Kashmir poses. The ideal way to deal with it would be taking measures that **not only addresses security but also developmental and sentimental concerns** of the people. It can be achieved by posting competent, motivated and humane police officers, armed personnel and administrators in militancy affected areas. To tackle local resistance tactfully, groups such as **'Village Defence Committees'** can be set up. This will also help denying support to Over Ground Workers (OGWs) to terrorist organizations. **Capacity Building** of State forces and local police should be done by providing them with proper training and equipment. Modernization and upgradation of state police infrastructure, weapons and technical equipment should be done. Further, lack of synergy between various agencies can be improved by bringing in greater coordination between central forces and state forces. Intelligence gathering mechanisms should be improved so as to have a better outcome. The control on the availability of explosives, drugs and counterfeit notes in the valley must be further tightened. Building technological infrastructure to target infiltration across the borders can go a long way in handling this crisis. **Smart Border Management system**, Integrated Law Enforcement Centers, smart walls can stop border infiltration to a large extent. Advanced technologies such as sensors, high tech surveillance equipment can be used to target inhospitable terrains and borders.

Another point of focus must be on bringing **development** in the region. This can be achieved by building infrastructure such as all-weather roads, bridges, railways, broadband connectivity etc. Private investment in the area must be encouraged and proper incentives and assurance of security should be given to industries and businessmen. Boosting **hinterland connectivity** will also give opportunity to people from rural areas to have open debates, develop inclusive mindset and aspire for growth, prosperity and boost the standard of living. The Jammu and Kashmir revered as heaven on earth offers immense **tourism potential**. This can be harnessed by facilitating development of able skill sets such as interpersonal and communication skills, establishing multi-language learning centers etc.

To address threat of radicalization, promotion of inclusive ideas and modern education should be pursued right from childhood through appropriate school curriculum. **Cultural interaction** of Kashmiri children and youths with the rest of the country with help of schemes such as **Ek Bharat Shrestha Bharat** should be promoted to build upon the understanding of each other's religion, culture, language, cuisines, art etc. Deradicalization measures should be adopted. Further, with acculturation of values like tolerance and mutual respect for other persons' religion, the issues in Kashmiri pandits rehabilitation and return can be addressed in a fundamental way. This will also put an end to communal and political debates portraying Kashmiris in bad light in the rest of the country.

Measures should also be undertaken to skill youth at mass level so that they can have better income opportunities. This will accelerate socio-economic development in a holistic manner and will reduce the inclination towards violence and also help in reducing income inequalities. **Back to Village (B2V) programme** is another step in a positive direction. The programme aims to involve the people of the state and government officials in a joint effort to deliver the mission of equitable development. It also aims to energize Panchayats and use community participation to direct development efforts in rural areas. Political vacuum which arises due to lack of timely election at local and state level can be solved by encouraging youths to enter politics. This can be achieved by trying to achieve effective **decentralization of powers** at local level and promotion of participative democracy in the region. Proper usage of **73rd and 74th Constitutional Amendment Acts** will ensure that grievances of common man, youth and other vulnerable sections are addressed which will further reduce the appeal of militancy. At the state level, political parties must share the responsibility to strengthen democratic values and culture. Problems should be resolved with discussion, debate and deliberation between various stakeholders. Developments such as the first ever **district development council elections** (November-December 2020) after abrogation of Article 370 are a positive development. In the

India-Pakistan Cricket Match and Kashmir

Cricket has been used a diplomatic tool in India-Pakistan ties, sometimes as part of track-II diplomacy or on other occasions to reflect disenchantment and disruption in relations. India-Pakistan cricket matches are also occasions when emotions of cricket fans run high. The cricket match sometimes seems like a proxy war between the two countries, with much more at stake than a win or loss in a sport. At occasions we hear in news of **celebration of Pakistan's win** or slogans in support of Pakistan creating communal conflict. Kashmiri students spread in college campuses across India have sometimes been at center of such conflicts. For example, during **the 2020 T20 world cup**, several such incidents from colleges in Sangrur in Punjab to Agra in Uttar Pradesh came up which involved fights between students from Kashmir and other states following bursting of crackers and cheering for Pakistan as Pakistan beat India in the match. Some incidents were settled after mediation and apologies, others saw Kashmiri and non-Kashmiri students ending up in police custody for crimes like creating communal enmity (section 153A of IPC), incitement to offence (section 505 of IPC) or booked under the National Security Act. Many such students got suspended from their colleges as well. Largely, such incidents end up creating trust deficit between Kashmiris and the people from other states of the country.

elections, the Gupkar Alliance emerged victorious on a majority of the seats while Bharatiya Janata Party, with 75 seats, became the single largest party.

One of the factors contributing to militancy has been the perceived human rights violations by the security forces due to extraordinary powers given to them under **Armed Forces Special Powers Act (AFSPA)**. Although it is vital for controlling militancy in disturbed areas, cases of misuse of powers under AFSPA have also been reported. Such cases should be dealt strictly and promptly to ensure justice to the victims. Government should also work on sensitization of the forces to project a humane face. Timely review of AFSPA to make it less obstructive of day-to-day life should be explored. Presently, a large number of youths have been recruited in police forces of Kashmir which is a welcome step.

Further, the historical linkages of the problem with Pakistan require efforts for bilateral deliberations. Thus, doors of **bilateral peace talks** without involvement of any third party should be kept open. It should also be kept in mind that Pakistan's agenda of internationalization of the Kashmir issue be curbed holistically so that it does not use terrorism as a tool for diplomacy. This can be achieved by calibrating and maintaining alliances at international level in favor of India's interest, exposing the role of Pakistan in causing unrest, violence and terrorism in Kashmir and elsewhere and international isolation of Pakistan. In long term, economic co-operation and integration should be pursued for creating constructive stakes in peace. SAARC as a regional institution could be used to achieve such an end.

Further, **broader diplomatic engagement should be done with Taliban** so that the soil of Afghanistan and fighters of Taliban are not used to create disturbance in Kashmir. Diplomatic convergence should be built on adopting the **Comprehensive Convention on International Terrorism (CCIT)** in interest of a common global strategy against use of terrorism as instrument of state policy.

Kashmir has a legacy and heritage of plural culture. Abrogation of Article 370 has politically integrated Kashmir with the rest of the country. But to find a solution to the Kashmir issue, all stakeholders must be taken into consideration. The issue of political vacuum within Jammu and Kashmir due to lack of elected government can be exploited by separatists and terrorist groups. Thus, timely conduct of elections after completing the delimitation process in uncontroversial manner is of crucial importance for promoting democratic ethos and constitutional spirit in a troubled region. It has now become all the more important to restore the diminished faith of the people in the democratic structures. As the biggest constitutional hindrance to J&K's assimilation stands removed, it is the duty of the Centre to bring people of J&K on board the common constitutional pathway and win over the confidence of the people through good governance. Alongside the emphasis on building bridges with the people, development of infrastructure, weeding out corruption from the administration, and reducing militancy and radicalization should be sought relentlessly.

The need today is for not only political but emotional integration of Kashmir and Kashmiri people with the rest of the country. The Vajpayee doctrine on Kashmir which was based on **'Insaniyat'** (humanity), **'Jamhuriyat'** (democracy), and **'Kashmiriyat'** (the ethos of Kashmir) cannot have an alternative. The spirit of universal acceptance as expressed by the former Prime Minister should be the light that would guide the national policy on Jammu and Kashmir.

Insurgency in North-East

6.1. INTRODUCTION: WHAT IS INSURGENCY?

Insurgency is an **organized armed struggle** by a section of the population against the state, often with foreign support. Possible causes of an insurgency include ideological, ethnic or linguistic differences; politico-socio-economic reasons and/ or influence of fundamentalism and extremism. Interference by external forces may act as a catalyst in providing a strong impetus to the insurgency movements. There are many examples of insurgency in India. For instance, in the state of Nagaland, the National Socialist Council of Nagaland (NSCN-Isak-Muivah) and National Socialist Council of Nagaland (Khaplang), the two insurgent groups are fighting to create a Greater Nagaland. In the state of Assam, Bodo rebel groups are fighting to establish Bodoland, etc. The goals of insurgent groups may be seizure of power, replacement of the existing regime and/ or liberation of a defined area from a supposedly oppressive rule.

About North East India

Geography of North East: North-east India is the easternmost part of India. It is connected to the Indian mainland via a narrow corridor sandwiched between the nations of Bhutan and Bangladesh. The narrow tract of land connecting the north-east with the rest of the country is known as **Siliguri Corridor**, sometimes also referred to as India's **'chicken neck' dilemma.** The Northeastern parts of India comprise of Sikkim and the seven contiguous states (seven sisters) of Arunachal Pradesh, Assam, Manipur, Meghalaya, Mizoram, Nagaland and Tripura. This region is home to 3.8% of the total national population and makes up about 8% of India's total geographical area.

Strategic relevance of Northeast: The North-east region plays **an important role in foreign policy**. The region shares a border with Bhutan, China, Myanmar, and Bangladesh and acts as a gateway to the Southeast Asian region (ASEAN countries) On account of its geographical position, the north-east holds significant **economic and trade potential**. North-east India is blessed with natural resources (oil, gas, coal, hydro, fertile land, etc.) which can be exploited for economic growth, development and connectivity. The region is also significant and is many times in news due to threats to territorial integrity of the country on account of **Chinese incursions** and claims in the region, particularly on Arunachal Pradesh. Thus, the region is critical in conserving the nation's territorial sovereignty. The fact that this region makes up around 40% of India's land borders with neighboring countries makes it vulnerable to infiltration of insurgents and militancy due to porous and open borders.

Cultural and ethnic diversity: The tribes living in India and those living on the other side of the border in neighboring countries have cultural and ethnic ties. For example, Naga tribes living in India and Myanmar have more cultural and ethnic similarities between them than with other tribes living within the same Indian state. The northeastern states are inhabited with diverse range of tribes. These states are not having a homogenous population rather they have a diverse set of cultures with ethnic and linguistic

differences in a small region, which makes them unique in their own way, for example culture and ethnicity vary between people living in valley and in hills of the same state. Such differences are also at roots of ethnic conflicts between tribes. Certain provisions of the constitution like Article 371, fifth schedule, sixth schedule provide autonomy to this region and its various tribes so as to conserve their culture and way of life.

6.2. BACKGROUND OF INSURGENCY IN NORTH-EAST INDIA

The roots of insurgency in the North-Eastern region of India are embedded in its geography, history, and a host of socio-economic factors. The conflicts in the northeast region range from insurgency for secession to insurgency for autonomy; from 'sponsored terrorism' to ethnic clashes, and conflicts due to the continuous inflow of immigrants from across the borders as well as from other States. The conflicts in the region can be broadly grouped under the following categories: (i) **National conflicts**: Involving the concept of a distinct 'homeland' as a separate nation and pursuit of the realization of that goal by its votaries. (ii) **Ethnic conflicts:** Involving assertion of numerically smaller and less dominant tribal groups against the political and cultural hold of the dominant tribal group. In Assam, this also takes the form of tension between local and migrant communities. (iii) **Sub-regional conflicts:** Involving movements that ask for recognition of sub-regional aspirations and often come in direct conflict with the State Governments or even the autonomous Councils.

These conflicts have led to widespread feelings of exploitation and alienation among the people in the northeastern region of India. Further, the failure of the Indian administration to cater to the demands of the people and to provide security on the ground has created a vacuum that is often filled by the various insurgent groups. These groups act as ethnic militia who also collect taxes and tolls, thus asserting their legitimacy among the people. The militia claim to provide for the security and assertion of the traditional rights, claims and laws of the tribes in the region. Moreover, there have been

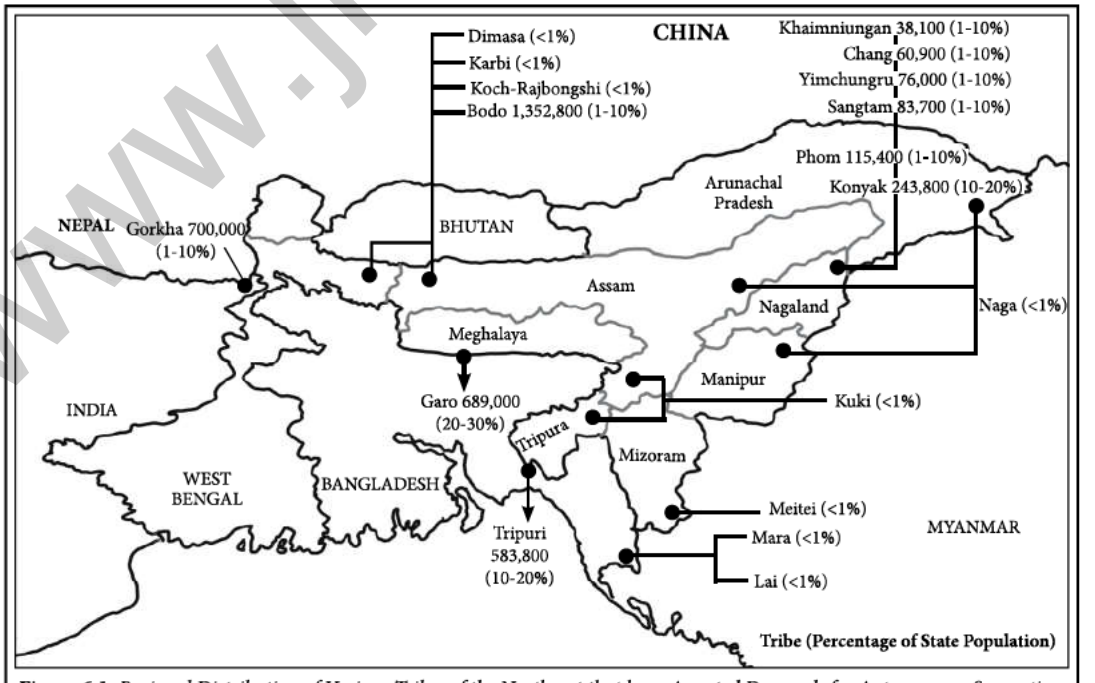


Figure 6.1: *Regional Distribution of Various Tribes of the Northeast that have Asserted Demands for Autonomy or Separatism*

instances of excesses committed by the security forces in the region which further fuels the claim of these insurgent groups as representing local tribal interests. The insurgent groups often indulge in unlawful activities such as damaging public properties, bomb explosions, extortions, the killing of innocent civilians and security forces personnel, attacks on or abduction of government employees, politicians, and businessmen, etc. Further, these organizations also maintain cross-border and international linkages to procure arms, smuggle drugs, access safe havens and for recruitment and training of their cadre.

6.2.1. Nagaland

The main demand of the insurgent movements in Nagaland is separation from India and the creation of a **Greater Nagalim** state which would extend across many Indian states and Myanmar's territories. The movement is led by Naga tribal groups, who are hill people of the region belonging to the Indo-Mongoloid family of the tribe. The Nagas are not a monolithic tribe, rather it is an umbrella term used for numerous tribes belonging to Nagaland and its neighboring areas in Manipur, Arunachal Pradesh, Assam, and Myanmar.

The Naga insurgency in the Northeast region has its roots in the long political history of the region. The Naga hills came under British India formally in the year 1866. The British followed the policy of non-interference in the administration of the Naga hills area. Consequently, Naga hills remained largely isolated from the events in the Indian mainstream and people residing in this area never identified themselves as 'Indians'. This legacy, in time, encouraged the educated Naga people to think about independence.

Later, the Nagas were recruited by the British to fight for them in **World War - I and II**. The Naga soldiers who returned from those wars picked up not only warfare techniques but also brought with them ideas of the French and American Revolution like Liberty, Equality, and Fraternity. Some of these Naga people later formed a club known as 'Naga Club' in 1918 to discuss their problems with the British. In 1929, they proposed their demand for sovereignty before the **Simon Commission**, which was prompted by determination to protect their traditional way of life based on customary laws. Although the colonial British Indian government did not agree to it, they realized that the tribal regions would need a special administration, and thus in 1937, the Naga hill districts along with the North-East Frontier Tract, the Lushai and North Cachar Hills were declared as **"Excluded Areas" in the province of Assam**. But this move failed to satisfy the demands of some Naga leaders. Later, the Naga Club was transformed into **the Naga National**

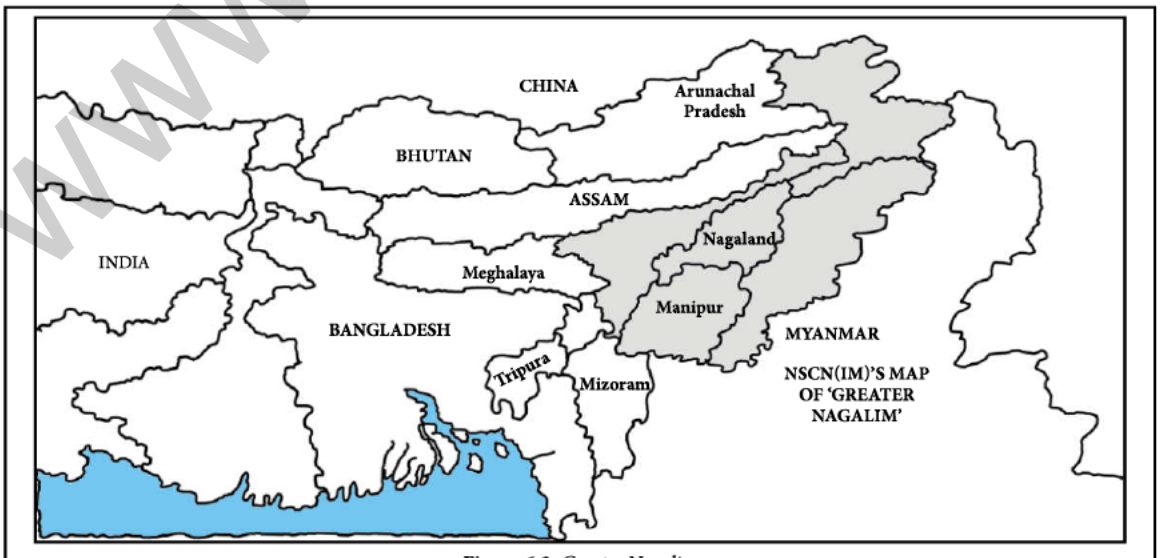


Figure 6.2: *Greater Nagalim*

Council (NNC) in 1946. It asserted opposition to the integration of Naga areas within the state of Assam. Under the leadership of Angami Zapu Phizo (A Z Phizo), the NNC declared Nagaland as an independent state on August 14, 1947. The then PM Nehru sent Sir Akbar Hydari, the Governor of Assam to discuss the issue with the Naga leaders. A nine-point agreement was signed between Naga leaders and the governor of Assam. However, the Government of India argued that the demands of Nagas were fulfilled under the constitution. This led to resentment among Nagas. This stage marked the genesis of Naga insurgency which was initially led by the Naga leader A Z Phizo who formed an underground Naga Federal Government (NFG) and a Naga Federal Army.

To counter the threat, the Government of India enacted the Armed Forces (Special Powers) Act (AFSPA) in 1958. Later negotiations began which resulted in separate **statehood for Nagaland** in 1963. However, by this time, use of force by the Indian state on Nagas had caused resentment among locals which fueled the voice of separatism. In 1975, a peace agreement called the **Shillong Accord** was signed, wherein the top Naga leaders decided to give up arms and join civilian politics. Still, some factions continued the secessionist movement and formed the group called the National Socialist Council of Nagaland (NSCN). Over time, many factions developed in this group with the two main factions being the NSCN (Issac & Muviah) and NSCN (Khaplang). The government has held talks with these groups over the years.

Armed Forces (Special Powers) Act (AFSPA) 1958

AFSPA is a legislation that grants special powers to the Indian security forces in areas declared as **'disturbed areas'** by the Union government or the governor of a state. The objective of the AFSPA is to counter any threat to territorial integrity by maintaining law and order in disturbed areas. Under the law, security forces can **'arrest a person without a warrant'**, who has committed or is even about to commit a cognizable offense, based on reasonable suspicion . It gives powers to the army, state, and central police forces to shoot, search houses and destroy any property that is likely to be used by insurgents in disturbed areas. The act also provides security forces with legal immunity for their actions in disturbed areas. As of January 2022, AFSPA* is in force in **Manipur, Nagaland, Assam, and Arunachal Pradesh**.

Criticism of AFSPA:

The overriding powers and immunities to the Armed forces under the AFSPA have been a subject of criticism. The act has **colonial and authoritarian roots.** AFSPA was originally brought in as an ordinance by the British in 1942 to suppress the Quit India movement. Although the act was retained after-independence to control partition-related violence for one year, it remained applicable till 1957, when the ordinance was turned into a permanent act of the parliament in 1958 due to uncontrollable violence in Assam and Manipur. The act has since remained applicable in perpetuity in many regions giving India the moniker of being among the few countries that resort to martial law like provisions in peace time. With the act giving absolute powers to the security personnel to aid the security operations, the actions under it are sometimes seen to be arbitrary in nature. For example, the **killing of coal miners as mistaken extremists** in Nagaland in December 2021 reflected an apparent lack of accountability. The lack of accountability in such incidents has been criticized by Supreme Court in a 2016 judgement which ruled against absolute immunity from investigation for actions committed under AFSPA. The act is believed as disruptive by local population and experts. **Irom Sharmila** fasted for 16 years for removal of AFSPA in Manipur. AFSPA is also said to be violative of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Convention against Torture.

But despite these issues, **AFSPA has proved to be of critical help** over the years. The overriding powers of the forces under the act allow for immediate action, situation control and restoration of order in insurgency affected areas. Special challenges like the support from external actors like China or the **porous borders** could not be addressed without special powers for the security forces. With improvements in security situation, AFSPA has been repealed from Meghalaya (1991-2018),

Tripura (1997-2015) and Imphal Municipal Area (1958-2004) in Manipur. In areas that continue to be affected by insurgencies, the act plays a vital role in controlling anti-state activities like arms smuggling or the illegal taxation and extortions by the insurgent groups. Peace and security maintained due to AFSPA has caused **developmental integration of the 'disturbed areas'** with the rest of the country. Increased build-up of infrastructure in recent years like the Dhola-Sadiya bridge in Assam which is the longest water bridge in India or the ongoing Jiribam-Imphal railway project with world's tallest railway bridge pier in Manipur could not have been envisaged without the security provided by AFSPA.

*Separate AFSPA was enacted for Punjab in 1983 (repealed in 1997) and for J&K in 1990 (still applicable).

Q. Human right activists constantly highlight the fact that the Armed forces (Special Powers) Act, 1958 (AFSPA) is a draconian act leading to cases of human right abuses by security forces. What sections of AFSPA are opposed by the activists. Critically evaluate the requirement with reference to the view held by Apex Court. **(UPSC 2015)**

Unlawful Activities (Prevention) Act, 1967 (UAPA)

UAPA is an anti-terror law aimed at effective dealing of certain unlawful activities of individuals and associations. The Act assigns absolute power to the Union government to deal with any terror-related issue. The act empowers the Union government to declare an activity as unlawful, by way of an **official Gazette**. The act has provisions for the death penalty and life imprisonment as the highest punishments. Under the act, both Indians as wells as foreign nationals can be charged. It will be applicable to an offender in the same way, even if the crime is committed on foreign land, outside India. The investigating agency can file a charge sheet within a maximum of 180 days after the arrests. Further, under the act, an organization can be proscribed as a terrorist organization and after the 2019 amendment in the act, even individuals can be declared terrorists under the act.

Both of these militant organizations signed a ceasefire agreement with the Union government in 2001. However, NSCN (K), the Myanmar based faction, broke the ceasefire agreement unilaterally in 2015 by killing 18 Indian soldiers and carrying out anti-social activities like extortion, political killings, etc. The government has currently classified NSCN (K) as a banned terrorist organization under the Unlawful Activity (Prevention) Act, (UAPA) 1967. The Union government, since 2017 has been engaged with several Naga organizations under the united banner of Naga National Political Groups (NNPGs) along with NSCN (IM) to amicably resolve the Naga aspirations. However, the major roadblock is the NSCN (IM) which has been alleged to sabotage the peace resolution process by trying to act as the sole representative of the Naga people and intransigence on **demands for a separate flag, constitution and territory** for a **Greater Nagalim**.

6.2.2. Manipur

The Insurgency in Manipur is part of the overall insurgency playing out in the Northeastern region of India It has elements of a secessionist movement as well as an ethnic conflict. The Kingdom of Manipur was conquered by the British following the Anglo-Manipur War of 1891, after which Manipur became a British protectorate. After the Independence of India, the Kingdom of Manipur was merged with the Indian Union on 15 October 1949. However, certain sections of the people who were loyal to the erstwhile King called it a **forced accession** and started insurgent activities against the established government. The alleged forced merger of Manipur and the delay in the conferring of full-fledged statehood to it was greatly resented by the people of Manipur. The first insurgent outfit to emerge in the State is the United National Liberation Front (UNLF) which was formed in 1964. After a protracted agitation, the region was given statehood in 1972. But over years, more insurgent outfits came into being, like the People's Revolutionary Party of Kangleipak (PREPAK) 1977, People's Liberation Army (PLA) in 1978, and the Kangleipak Communist Party (KCP in 1980 emerged in the Manipur valley areas consisting of four districts (Imphal West, Imphal East, Thoubal

and Bishnupur) of the State. These insurgent groups have been demanding a separate, independent state of Manipur.

Manipur also has a sizable population of **Nagas** in two districts of the state which leads to a similar pattern of insurgency as is prevalent in the state of Nagaland. The Naga insurgent groups active in these districts seek integration of these parts of Manipur under the Greater Nagalim. The demand for the merger of parts of Manipur in the Greater Nagalim has led to counter-mobilization of other Manipuri tribes like the **Meitei** who form the majority in the state or the **Kuki** among other tribes against the Nagas, leading to an inter-tribe rivalry. Further, Kuki tribes in the early 1990s initiated their insurgency against the alleged oppression by the NSCN-IM. Following ethnic clashes between the Nagas and Kukis in the early 1990s, a number of Kuki outfits were formed. Several other tribes, such as the Paite, Vaiphei, and Hmars have also established their own armed groups. Similarly, Islamist outfits like the People's United Liberation Front (PULF) have also been formed to protect the interests of the Manipuri Muslims.

The state in its entirety had been declared a 'disturbed area' under AFSPA in 1980 and the Armed Forces Special Power Act continues to be in place till now. The implementation of AFSPA resulted in alleged instances of use of excess force and indiscipline on part of the personnel in the armed forces giving rise to civic uprising, including the infamous **'mothers' nude protest'** and **Irom Sharmila's 16-year-long hunger strike** against the Act. The AFSPA is still embroiled in controversy and the people of Manipur continue to protest the imposition of AFSPA in the state.

Lastly, due to the problem of militancy, the investments meant for infrastructural development have been divested towards augmenting security to counter the growing threats to public safety in the state. The number of educated unemployed youths in the state has been growing and they become easy recruits for the militant outfits. The number of cases of extortion has also been increasing. Militants have resorted to extorting from almost all places including places of worship, educational institutes, health centers, and commercial establishments. This has led to the closure of quite a few establishments in the state and discourages businesses from coming into the state. The vicious cycle of economic backwardness creates a fertile ground for insurgent groups to inflate by recruiting youths from such regions.

6.2.3. Assam

The root cause of insurgency in Assam is said to be the immigration of 'non-natives' in the region. The influx of immigrants started under British rule had started creating a demographic shift in the region. The British had distinct policies for two parts of Assam: Tribal highlands and plains. For highlands, it maintained a policy of relative isolation and here the population was ethnic Assamese, they classified this as a tribal area. In contrast, lowlands or plains were largely Hindi-speaking; this was a non-tribal area and was fully exploited by the British. In these areas, the British administration relied completely on immigrants for labor who were largely **Bengalis, Bihari,** and **Non-Bengali Muslims**. After independence, there was a continuous influx of illegal immigrants from Bangladesh. This flow of population over time gave the Assamese population a kind of cosmopolitan character similar to any other big city of India. But this demographic dynamism also started simmering discontent among the 'native' Assamese population who felt themselves to be at a disadvantage due to the influx of immigrants. In the 1970s, there was a series of agitations which was spearheaded by the **All-Assam Students Union (AASU)**, a student organization, which started a non-violent satyagraha and boycotts to demand deportation of illegal immigrants who had emigrated from Bangladesh to Assam. Later, these protests turned violent when it appeared that illegal migrants have gotten into electoral rolls and local Assamese parties would now lose elections. This resentment led to the creation of the **United Liberation Front of Assam (ULFA)** and some other similar militant groups. ULFA emerged as the main militant organization in Assam with two objectives: a) carve out an independent Assam state and b) rule it on socialist lines. The violence was resolved through an agreement between the representatives

of the Government of India and the leaders of the Assam Movement as the **Assam Accord** in **1985**. Subsequently, the **Asom Gana Parishad (AGP),** the regional political party that was formed by the AASU leadership, won the elections to form the government in Assam showcasing the widespread support for the movement. However, ULFA did not acknowledge the Assam accord.

Assam Accord, 1985

The Assam Accord (1985) was a **Memorandum of Settlement (MoS)** signed between representatives of the Government of India and the leaders of the Assam Movement on 15 August 1985. The accord brought an end to the violence that started in Assam in the late 1970s. Under the accord, all those foreigners who had entered Assam between 1951 and 1961 were to be given full citizenship, including the right to vote. Those foreigners who had entered Assam after 1971 were to be deported; the entrants between 1961 and 1971 were to be **denied voting rights for ten years** but would enjoy all other rights of citizenship. Further, under the accord, the Union government also promised to provide legislative and administrative safeguards to protect the cultural, social, and linguistic identity and heritage of the Assamese people.

The ULFA continued to carry out attacks on Indian security forces and when Indian forces used to retaliate the ULFA militants would escape across the porous border to Bhutan or Bangladesh. Because of ULFA's increased presence in Assam, the Union government outlawed the group in 1986 and declared Assam a troubled area. Later, New Delhi pressured Bhutan to carry out operations to drive out the ULFA militants from Bhutanese territory. The Bhutanese army backed by the Indian army successfully eliminated several hideouts of the ULFA along the Bhutan border. Since then, the support for the militant group has continued to dwindle. But the organization continues to pose a considerable threat to peace and security in the state due to which the Union government has proscribed ULFA as a banned terrorist organization under the **Unlawful Activities (Prevention) Act (UAPA), 1967.** The demand of ULFA and other organizations for political autonomy in Assam led to the counter mobilization of another Assamese Ethnic group, called Bodos. They formed the **All-Bodo Student Union** and escalated violence against ethnic Assamese people. They also raised the demand for a separate state Bodoland but the demand could not be fulfilled because no ethnic group is in the region is in an outright majority. The Union government negotiated with the Bodo leader to find an amicable solution and as a result, the government offered to constitute the **Bodo Territorial Council** under the sixth schedule of the Indian constitution. Later, a Bodo militant organization was formed in 1998 called the **National Democratic Front of Bodoland (NDFB)** which seeks to establish a sovereign Bodoland. The group has carried out several attacks on civilians in Assam, targeting non-Bodo civilians and the security forces. Although in May 2005, NDFB signed a ceasefire agreement with the Union government, some of its factions continue to indulge in militancy. The group continues to be (as of 2021), proscribed as a banned terrorist organization under the UAPA1967.

Sixth Schedule of Indian Constitution

The sixth schedule was added in the Indian constitution to protect tribal populations of the northeast state of Assam, Meghalaya, Tripura, and Mizoram and provide autonomy to the tribal communities in these states through the creation of **Autonomous District Council (ADC)** that can frame laws on land, public health, agriculture and others. As of now, 10 autonomous councils exist in Assam (3), Meghalaya (3), Tripura (1), and Mizoram (3). The ADCs administer the areas under their jurisdiction. The ADC can make laws on certain specified matters like land, village administration, inheritance of property, marriage, forests, canal water, shifting cultivation, divorce, social customs and so on. However, all such laws made by ADCs require the assent of the governor.

Further in the Karbi Anglong region of Assam, there is the prevalence of violent conflict between the dominant Karbi tribe and the other tribes in the region. It includes violent clashes between the ethnic insurgent **Karbi People's Liberation**

Tigers (KPLT) and the **Rengma Naga Hills Protection Force (RNHPF)** in Karbi Anglong district of Assam which has forced thousands of people from the Karbi and Rengma Naga tribes to leave their homes. The KPLT is an off-shoot of the ethnic insurgent **Karbi Longri North Cachar Hills Liberation Front (KLNLF),** formed in 2011. The KLNLF is demanding a separate State comprising two hill districts of Karbi Anglong and Dima Hasao. KLNLF is now engaged in talks with the Centre and the State government. When the KLNLF signed the Suspension of Operation agreement with the Centre and the Assam government, about 20 cadres of the outfit parted ways and formed the KPLT in 2010. The KPLT has been demanding the creation of a self-ruled homeland for the Karbi people. The RNHPF was formed in 2012 for the protection of the Rengma Nagas from KPLT attacks. The outfit has been demanding the creation of a regional council for the Rengma Nagas of Karbi Anglong district of Assam.

6.2.4. Mizoram

The insurgency resolution of Mizoram is one of the most notable successes of the Indian establishment in northeast India and acts as a guiding light for the peaceful resolution of insurgency in the region. The insurgency in Mizoram had its genesis in the late 1950's famine that hit the Mizoram region. The Indian government failed to provide adequate relief to the masses in Mizoram during the famine which caused resentment among the local population. The situation was further aggravated by some groups that mobilized locals on the basis of the Mizo ethnic identity. The movement was led by **Mizo National Front (MNF),** which had racial and religious overtones. The MNF declared the secession of Mizoram from the Indian Union its primary objective. There was an armed uprising that started in 1966 and violent conflict continued up to two decades well into the 1980s., The MNF started running its own parallel administration in areas of Mizoram and it was assisted by Pakistan, which supplied arms and ammunition to the MNF through the then east Pakistan region (which would later become Bangladesh). However, after arduous negotiations, the **Mizoram Accord of June 1986** was signed under the leadership of the then PM Rajiv Gandhi and the MNF leader **Pu Laldenga,** which succeeded in bringing the violent conflict of the past decades to a peaceful and satisfactory end. The maturity displayed by the two Mizo political personalities of the time, namely, the undisputed insurgent leader Pu Laldenga and the then Chief Minister **Pu Lal Thanhawala** ensured a peaceful transition to peace in the region. Further, the then Chief Minister Pu Lal Thanhawala's unilaterally offered to step down in favor of Laldenga as the chief minister had a moderating influence and there was pressure of the Mizo civil society, especially the women who had been the most aggrieved and affected during the periods of violence. Under the agreement, the MNF rebels laid down their arms and were granted amnesty against prosecution by the Indian Government. The government agreed to grant full statehood to Mizoram, and Laldenga himself assumed office as chief minister. The agreement raised the prospect of the return of peace to the state of Mizoram. The leaders of MNF made a spectacular transition; from once being insurgents in the jungle to politicians in the secretariat put there by votes of the people.

6.2.5. Tripura

Tripura, just like other states in the northeast, had been infested with insurgency. The insurgency in the state resulted from both politico-historical as well as ethnic tensions. The ethnic rivalries arose because of the immigration of Bengali-speaking people from East Bengal who pushed the native Tripuri people towards the hilly and under-developed regions of Tripura. The politico-historical tensions have their genesis in the unification of Tripura with the newly independent India. Some groups allege that the Tripura monarch was forced into the unification and thus native Tripuri people have been subjected to unfavorable terms. It is because of these two major factors that Tripura witnessed a surge in terrorist activities in the 1990s. But the beginning of the insurgency in Tripura can be traced to the formation of the **Tripura Upajati Juba Samiti (TUJS)** in 1971, which was followed by the Tripura National Volunteers (TNV) in 1981. The National Liberation Front of Tripura (NLFT) was formed on March 2, 1989, along with its armed

wing, the National Holy Army. The objective of NLFT is to secede Tripura from India and lay down the foundation of an independent Tripuri state and deport all 'illegal' Bengali immigrants from its territory along with the implementation of the Tripura merger agreement and the restoration of land to the tribal people under the Tripura Land Reform Act, 1960. Another militant organization All Tripura Tiger Force (ATTF) was established in July 1990 with similar objective as those of NLFT, however, ATTF did not seek to secede Tripura from India. Presently as of 2021, both ATTF and NLFT are proscribed in India as terrorist organizations under the Unlawful Activities (Prevention) Act, 1967. Till, 1995, the insurgency in Tripura remained low profile, but the unrest grew in magnitude between 1996 and 2004. The reasons for success of insurgency during this phase was due to the advantages of the rough, rugged terrain, and the porous and extensive trans-border corridors with Bangladesh. Safe havens in Bangladesh, logistic support from the then supportive Bangladesh establishment, and networking with potential insurgent outfits aided the sustenance of insurgency. A build-up of weapons, explosives, and wireless communication systems, and extortion and 'levies' fueled the volatile insurgency. However, the insurgency started waning after 2004, as the state government addressed the problems in a strategic and resolute manner under the leadership of the then Chief Minister Manik Sarkar. Later, the initiative of the Union government to increase the area under the control of the **Tripura Tribal Areas Autonomous District Council** after a tripartite agreement between the Union, the state government, and the Council was able to meet the demands of disgruntled masses. The government has since brought the insurgency under control, and has so far succeeded in limiting extremist activities. Just like Mizoram, Tripura has also scripted a story of triumph over insurgency and conflict-resolution and demonstrated that insurgency is not an insurmountable problem.

6.2.6. Arunachal Pradesh

The insurgency in Arunachal Pradesh is because of the presence of insurgent organizations like NSCN (IM) and (K), ULFA and Naxalites. The two NSCN factions exist in the three districts of **Tirap, Changlang, and Longding in Arunachal Pradesh**, as the NSCN factions claim these areas under their demand for Greater Nagalim. ULFA and Naxalite use Arunachal Pradesh as means of transit while escaping from Indian security forces towards their safe havens in Myanmar. These militant organizations carry out extortion, drugs, and arms smuggling activities to fund their activities which are against Indian interests. The action by Indian security forces has been successful in keeping the violence in Arunachal Pradesh under check, but still, these organizations continue to work in the state maintaining a low-profile. Further, the resettlement of **Chakma and Hajong refugees** in Arunachal Pradesh has created discontent among the local tribes of Arunachal Pradesh as they fear being marginalized by the existence of these groups. This fear has at times led to sporadic violence in the state. However, the Union government have taken steps to assuage the fear of the local population by considering their demands like for example the exemptions for the Inner-line permit areas and the areas under the sixth schedule of the Constitution (parts of Assam, Meghalaya, Tripura, and Mizoram) under the **Citizenship Amendment Act (CAA), 2019** which seeks to provide expedited citizenship to the persecuted religious minorities from the three neighboring countries of Afghanistan, Bangladesh, and Pakistan who migrated to India on or before 31st December 2014.

Inner Line Permit (ILP)

ILP is a document issued by the state government under the ILP system, which allows non-natives to visit or stay in a region under ILP system for a certain period of time. At present, 4 Northeastern states have ILP, namely, **Arunachal Pradesh, Mizoram, Manipur, and Nagaland**. Both the duration of stay and the areas allowed to be accessed for any non-native are determined by the ILP. The Inner Line Permit draws its legal backing from the **Bengal Eastern Frontier Regulation Act 1873**. ILP came into existence to safeguard the demographics of a region especially the tribal areas of northeast India.

6.2.7. Meghalaya

The insurgency in Meghalaya is marked by the mobilization of tribal people along ethnic lines of

division. The militant organizations that have been active in the state include Garo National Liberation Army (GNLA), Achik National Volunteer Council (ANVC), and Hynniewtrep National Liberation Council (HNLC). All these organizations have their own distinct agendas. The ANVC was formed in 1995 with the objective of forming an Achik Land in the Garo Hills. As of now, a **Suspension of Operations Agreement** between the Government and ANVC has been in force since July 23, 2004. Later in 2014, a tripartite agreement between the Union government, the State government, and the ANVC led to the dissolution of the group. The GNLA seeks to establish a separate **Garoland for the Garo people**. The organization was formed in 2009 and consists of members, drawn from other militant organizations active in and around the state. Presently, GNLA is a proscribed as a terrorist organization under the Unlawful Activities (Prevention) Act, 1967. The HNLC was formed in Meghalaya in 1992. The organization claims to be a representative of the Khasi-Jaintia tribal people, and its aim is to free Meghalaya from the alleged domination of the Garos and the non-tribal outsiders (Dkhars). HNLC was banned by the Union government in 2000. These militant organizations are involved in carrying out activities like **kidnapping, extortion, political killings**, etc. to fund their cause and to extend their philosophy.

6.2.8. Sikkim

Sikkim is an exception in the Northeast landscape when it comes to insurgencies. Unlike other states in the northeast, Sikkim has never witnessed any instance of insurgency or major ethnic conflicts. The peaceful situation in the state can be attributed to well-crafted constitutional mandate of striking a balance between the various ethnic groups (primarily the Lepchas, Bhutiyas, and Nepalis) that has prevented the emergence of a major ethnic or political conflict.

Q. The north-eastern region of India has been infested with insurgency for a very long time. Analyze the major reasons for the survival of armed insurgency in this region. **(UPSC 2017)**

6.3. Role of Neighboring Countries

6.3.1. Bhutan

India has porous borders with Bhutan and for a long time, the militant groups in the northeast region, especially groups active in Assam had been taking refuge in Bhutanese territory to escape counter-insurgency measures by Indian security forces. In a bid to control insurgency in the Assam region, India launched **Operation Rhino** and **Operation Bajrang** against ULFA in 1990. Facing strong pressure, Assamese militants relocated their camps to Bhutan. It was difficult for Indian security forces to counter these groups operating from Bhutan. Thousands of cadres of the ULFA and more than a thousand Bodo militants from Assam were estimated to have crossed the borders and were settled in camps in southern Bhutan. Bhutan cooperated with India in uprooting the militant groups from its soil. For example, **Operation All Clear** was a military operation conducted by Royal Bhutan Army during 2003-04 against Assam's separatist insurgent groups. Bhutan has repeatedly reassured India that it would launch operations to flush out anti-India insurgents which operate from Bhutanese soil.

6.3.2. China

According to reports of Indian intelligence agencies, China has supported insurgents in the northeast since early 1960s and continued the support through later years too. In May 1966, Nagas approached the People's Republic of China assistance. The Naga fighters were given physical and tactical training in weapons, guerrilla warfare etc. and ideological training in Maoism in neighboring Chinese province of Yunnan. The motive behind China's support to insurgent forces in the northeastern states is to weaken India from within, take advantage of the disturbed situation and get control over Indian territories. There are border disputes between India and China in the region as China continues to contest Indian sovereignty over large parts of Arunachal Pradesh. In November 2021, a number of reports including from Pentagon in USA claimed that China had constructed villages in border regions of Arunachal Pradesh. China also poses threat to the Siliguri

or 'the Chicken neck' corridor as seen in Doklam dispute in 2017.

Doklam Stand-off:

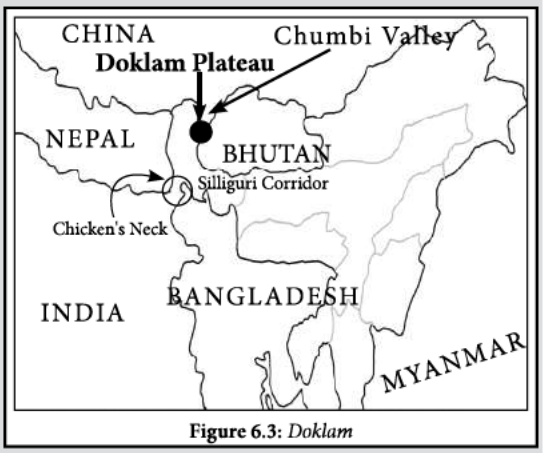


Figure 6.3: *Doklam*

In 2017, Indian and Chinese armies were locked in a stand-off situation in Doklam, a plateau region marking the border trijunction between India, China and Bhutan. India army blocked Chinese attempts to extend a road in the region. While the area is contested territory between China and Bhutan, increased Chinese presence in the area poses military threat to India's Siliguri Corridor that connects the larger part of the country with the north-eastern states. The nearly three-month long standoff situation was resolved with China agreeing to halt road construction in the area and both sides withdrawing forces.

6.3.3. Nepal

There is credible evidence available from investigation in terror incidents and organized crime to suggest that Nepal's territory has been used by Pakistan to fuel insurgency and terrorism in India. Nepal is used as a conduit for logistical support to smuggle in ISI agents, drugs, weapons and as an escape route for perpetrators of terrorism or related acts in India due to India's 1800 km long open border with Nepal. For example, Yakoob Memon, one of the main accused in the **Bombay Blast** case in 1996 was tracked down to Nepal's capital Kathmandu; the infamous **Kandahar hijacking of** Indian aircraft from Kathmandu in 1999 revealed the dangerous potential of cross-border intelligence activities conducted through Nepal to harm Indian security interests. In the context of north-east India, ISI agents or other international actors have found the Nepal route to be safe to enter into the northeast and other regions from where counterfeit Indian currency and weapons are supplied to the insurgents. But Nepal has over the years also cooperated with India in carrying out covert operations against anti-Indian activities such as the 2013 arrest of Yasin Bhatkal, co-founder of Indian Mujahideen. Further, both countries conduct a **joint military exercise 'Surya Kiran'** to fight with synergy in counter-insurgency and counter-terrorism.

6.3.4. Bangladesh

With the emergence of Bangladesh after the **India-Pakistan war of 1971**, the tribal insurgents operating under Pakistani intelligence cover within East Pakistan suffered a blow, and their number reduced under the regime of the then PM of Bangladesh **Sheikh Mujibur Rehman**. However, after his assassination, the new regime allowed the Mizo insurgents to establish their base in the Chittagong Hill Tracts. However, many experts opine that the current government of Bangladesh under **PM Sheikh Hasina** has been very keen on improving relations with India. In recent years, the Bangladeshi government has been cooperating with Indian Intelligence in flushing out anti-India militants from its territory. It has arrested several terrorists of insurgent groups like **ULFA, NSCN, BNDF**, etc., and extradited them to India. However, illegal migration from Bangladesh continues to pose a challenge to internal security. For example, it has been recently seen that members of the Arakan Rohingya Salvation Army which had been living in Bangladesh and found a safe haven there, had tried to infiltrate across the border to India. The porosity of the India-Bangladesh border makes the northeast a hotspot for large-scale migration. In 2018, the then Army Chief General Bipin Rawat characterized the illegal immigration from Bangladesh as a proxy warfare supported by Pakistan and China to keep the north east in a disturbed state. Such issues need to be addressed by both countries with joint cooperation. A **joint**

military exercise to promote defence co-operation between armies of the countries including counter-terrorism, counter-insurgency, and other challenges has begun between India-Bangladesh which is known as the **Sampriti** exercise, with the recent edition, the ninth iteration of the exercise, being conducted in Umroi, Meghalaya in 2020.

6.3.5. Myanmar

India shares a 1670 km long **porous land border** and a close **maritime proximity** with Myanmar. For instance, India's Landfall Island and Myanmar's Coco Island are just 40 km apart. The population living along the India-Myanmar land border has strong socio-cultural and **ethnic ties**. The Indo-Myanmar border remains comparatively peaceful and there is no major border conflict between the two countries. However, there continues to be separatist sentiments and legacy of discontent among the various tribes living along the borders on both sides. Many northeastern insurgent groups, like the **Nagas, the Mizos, and the Meitis**, have had bases in Myanmar taking advantage of the forested terrain. However, the Myanmar government has been cooperative with the Indian government including in checking the movement of militants across the border, strengthening the communication network along the international border, stepping up measures against **narcotics smuggling** across the border and conducting joint military operations against the militants operating out of Myanmar. For example, **'Operation Golden Bird'** of 1995 dealt a heavy blow to ULFA. In 2015, a surgical strike was conducted by Indian security forces along the border in Myanmar territory, where a number of base camps of Naga insurgents were destroyed. A joint operation against Arakan Army's militants in 2019 prevented a planned attack on the **Kaladan project** being jointly developed by the two countries in Myanmar.

Q1. Analyze internal security threats and transborder crimes along Myanmar, Bangladesh and Pakistan borders including Line of Control (LoC). Also discuss the role played by various security forces in this regard. **(UPSC 2020)**

Q2. Cross-Border movement of insurgents is only one of the several security challenges facing the policing of the border in North-East India. Examine the various challenges currently emanating across the India-Myanmar border. Also, discuss the steps to counter the challenges. **(UPSC 2019)**

Q3. India's proximity to two of the world's biggest illicit opium-growing states has enhanced her internal security concerns. Explain the linkages between drug trafficking and other illicit activities such as gunrunning, money laundering and human trafficking. What countermeasures should be taken to prevent the same? **(UPSC 2018)**

Q4. How does illegal transborder migration pose a threat to India's security? Discuss the strategies to curb this, bringing out the factors which give impetus to such migration. **(UPSC 2014)**

Q5. How far are India's internal security challenges linked with border management particularly in view of the long porous borders with most countries of South Asia and Myanmar? **(UPSC 2013)**

6.4. GOVERNMENT STEPS TO CURB INSURGENCY

The Union government has acknowledged the problems from conflicting demands of the diverse ethnic groups and has been following a policy of talks and negotiation with the insurgent groups that abjure violence, lay down arms, and seek solutions for their problems peacefully within the framework of the Constitution of India. As a result, a number of insurgent outfits have come to peace terms with the Government of India and have entered into **Suspension of Operations** agreements, some of them have signed **Memorandum of Settlement** and some groups have even dissolved themselves. At the same time, the militant groups which do not engage in talks are being dealt through counter-insurgency operations by the Indian security forces. To curb the unlawful activities of these insurgent

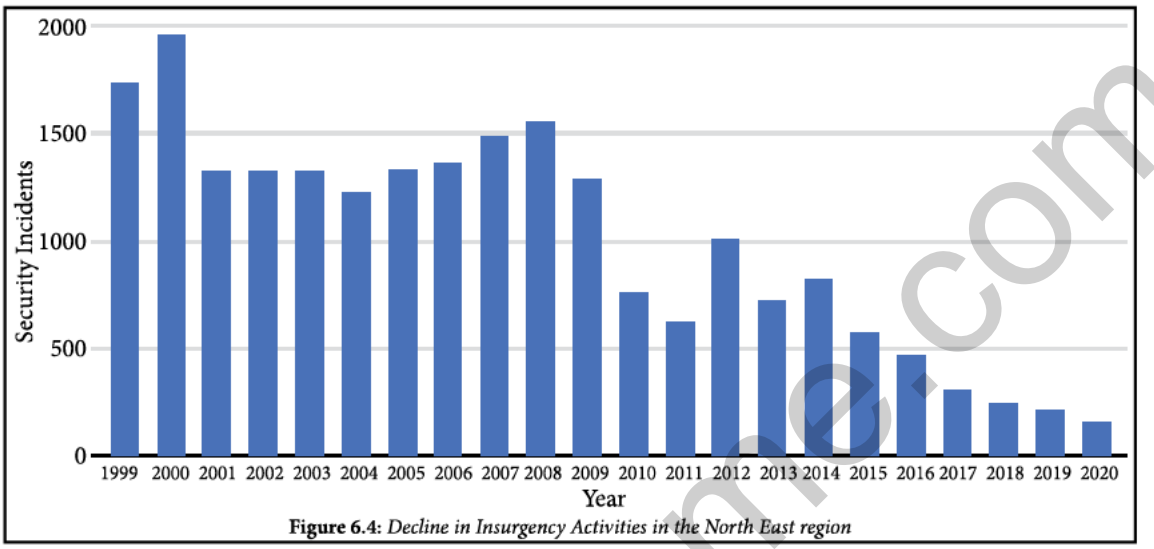


Figure 6.4: *Decline in Insurgency Activities in the North East region*

groups, the Union government bans such groups under the **UAPA, 1967**, thus, taking away the fundamental right to form associations under the specified reasonable restrictions for such outfits. To deal with the insurgency situations, the Union government from time to time also empowers the security forces with powers under **AFSPA**. The application of AFSPA has yielded successful results in Meghalaya and Tripura, as these states are now free from the insurgency and as a result have been removed from purview of AFSPA.

Although, law & order is a state subject, the Union government provides assistance to the states in law & order maintenance by deploying **CAPF (Central Armed Police Force)**. Further, the Union government has been running schemes like surrender-cum-rehabilitation of militants in north -east to encourage militants to give up violence and choose democratic and peaceful ways to push their demands. Under the scheme, the government is also providing monetary benefits to fund the self-employment ventures of militants who voluntarily give up arms. The government has also launched several policies and schemes for meeting the development needs of the people in the region. The **Department of Development of the Northeast Region** (also called DoNER) was established in 2001 by the central government to give exclusive focus to the development of the north-east India. Later it was upgraded to a full-fledged ministry in 2004 headed by a Cabinet Minister. The government is also trying to woo youth away from influence of insurgent outfits by engaging them in sports and extra circular activities. The government has also been promoting the Northeast as a tourist destination to increase employment opportunities in the state.

The above-mentioned figure shows recent trends of insurgency waning down in the northeastern states. The positive trend can be attributed to the fact that greater autonomy has been provided to the tribal societies through the autonomous district council, greater funds have been devolved for development of the region, including on infrastructure and connectivity. Better monitoring of development schemes in affected areas, fatigue in the insurgents and rehabilitation program of government for those willing to denounce violence has helped. The success of counter-insurgency operations resulting in loss of cadres, leaders, shortage of funds, arms and ammunition, arrests, surrender, desertion, and success of peace talks with the government are some other critical factors behind reducing incidents of insurgency in north-east.

6.5. WAY FORWARD

Though the objectives, demands of different insurgent groups in the northeast are different but the major underlying factors behind these insurgencies are assertion of ethnic identity and grievance against economic **under-development**.

Hence, certain steps are crucial to curb insurgency in the northeast. The Government of India believes that through a holistic approach focusing on development and security the issue of insurgency can be dealt with effectively.

In terms of **military action**, there is a need for greater coordination between central forces and state forces for a better tactical response to curb insurgency. State police and central forces should cooperate with each other to ensure effective intelligence sharing, investigation, and operations against militants. Further, the intelligence gathering mechanism needs to be improved and the intelligence gathered needs to be disseminated in a timely and actionable manner. Moreover, the government should also focus on coordinating operations with the neighboring countries to eliminate insurgent safe havens in the neighboring countries. Another notable reform could be with regards to AFSPA. It should be either reformed or repealed as it is one of the reasons for the spread of insurgency in the northeast as it is often alleged to be abused by the forces. The security forces can be sensitized to ensure the **protection of human rights**. Also, cases, where AFSPA have been abused, should be dealt with a heavy hand and the guilty should be punished. In **dialogue and negotiations** with insurgents, the pre-condition of complete abjuring of violence for holding peace talks is a possibly flawed notion as it may not always bring on board all insurgent groups. Dialogue with insurgents should be an ongoing process with enough flexibility to reach concrete solutions by involving all the stakeholders. Also, an iron hand approach should be used to deal with those insurgents who have performed acts of violence while providing surrender options to those who have given up arms. To further improve **border security**, a Smart Border Management system can be incorporated which can stop border infiltration and protect from insurgents which reside in neighboring countries. The comprehensive integrated border management system can be very beneficial in weeding out such insurgents. Capacity Building of State forces and local police should be done by providing them with proper training and equipment so as to ensure them to be primary protectors against any local insurgent activities.

The constitution of India addresses the uniqueness of northeast India through provisions for special **administrative and governance measures** and has fulfilled the demands of some insurgents by providing greater autonomy to some communities, groups and regions such as autonomy under the **sixth schedule** of the constitution, Panchayat (Extension to Scheduled Areas Act) or **PESA,** etc. These measures help communities to preserve their identity and culture while giving them greater autonomy in decision-making at the local level. However, this autonomy in local governance is meaningless in absence of adequate funds in the hands of such bodies for their smooth functioning. Improving administrative efficiency and providing people-centric governance to the people of the northeast may assuage feelings of discontent in the people. Also, the government needs to be prudent while making policies for the region. There should be no one-size-fits-all approach for the whole of North East. Moreover, policies made for dealing with the insurgent groups should win the hearts and minds of the people of the North East and should be based on the understanding of the root cause of insurgencies.

Economic development of the area should be done in a calibrated manner. The development should not only take into account the environmental fragility of the region but also should respect different customs and traditions of the people of the region for example, customary laws about communal ownership of land and resources etc. Any development in the region should be sustainable and should have the participation of the locals to ensure its acceptance by the locals. Also, there is a stark need to enhance communication and connectivity in the northeast for better developmental, economic and cultural integration of the region with the rest of the country. This would also help in the delivery of government services to people., Further, Special Economic Zones (SEZs) along or across the India-Bangladesh border and India-Myanmar border should be planned in collaboration with the government and civil society in neighboring countries. The proposed **logistic hub in Sabroom** in Tripura is a constructive initiative that should be built upon to build cross-border economic ties. It will not only generate revenues but also help in large-scale employment generation,

cutting off the roots of insurgency in north-east. **Skill development** schemes like the National Rural Livelihood Mission/ Deen Dayal Upadhyaya Antyodaya Yojana (DAY) should be aligned as per regional strengths and needs. Capacity-building measures are required. Cultivation of bamboo and forest produce along with related value addition is one example where focus on skilling can create globally renowned products. Marketing support for regional handicrafts, **geographical indication** support, promotion of **agricultural exports**, IT-hubs and **digitization infrastructure** can bring along skills in traditional and modern vocations at par with global demands. Increasing economic avenues will raise the standard of living and help meet the regional aspirations. **Tourism** can be a major fulcrum of economic prosperity in the region. The virgin beauty of nature in north-east remains under-explored by domestic as well as international tourists. The unique geography, ethnic diversity and tribal customs of the region can help tap into niche tourism opportunities, if supported by the right infrastructure. Tourism can not only be the source of revenue and economic gains but also a catalyst for promoting cultural integration.

There is also need to enhance cultural interaction of the north-east with the rest of the country to advance goals of **cultural sensitization** as a measure against racism. Currently, there is a sub-conscious alienation between Indians from 'mainland' and those from the virtual island of north-east India. This distance often gets manifested in forms of discrimination, stereotypes and casual racism. During the recent pandemic, incidents of slurs being thrown at people from north-east including calling them 'corona' came to light. In 2012, rumor mongering about racial targeting of people from north-east led to a near-exodus of northeastern people from Bengaluru. Measures to address such psychological distance between north-east and rest of the country can include socio-economic development that promotes inclusive outlook, sensitizing people about the northeastern states, the various tribal communities and their way of life, providing value-based education in schools and colleges so as make them tolerant towards all the section of the society, school-exchange programs etc. The **'Ek Bharat, Shreshtha Bharat' scheme** of government to promote understanding of culture, language, cuisine, the art of other states which is distinct from one's own state is a good initiative. The program aims to actively promote interaction between people of diverse cultures living in different states and UTs of the country, with the aim of promoting greater mutual understanding amongst them. Such programs can counter the parochial mindset of people regarding other people's cultures and ethnicity and curb feelings of supremacism about own community or ethnicity.

Lastly, **good relations with neighboring countries** have helped in curbing insurgency such as the joint military operations with Myanmar or increased sensitivity in Bangladesh about anti-India militant groups. The government should follow the success in security cooperation with initiatives for regional economic integration through groups like BIMSTEC. The Act East policy is right in its intent to make the north-east India's economic gateway to south-east Asia. But a rethink in approach may be needed to address lacunae in achieving the vision. Out-of-box solutions like open border policy, Comprehensive Economic Partnership Agreement, customs union etc. can help push the rise of north-east India as the regional economic hub. The government can also use the **Northeast council** to formulate plans to engage the ASEAN in the region's economy.

Act East Policy

The Act East policy was launched in 2014. The policy plays an important role in India's foreign policy towards east and south-east Asian countries. The focus of the Act East policy is on economic engagement with India's extended neighborhood in its east. at bilateral, regional, and multilateral levels. The policy lays emphasis on the northeast region of India as the gateway to the countries and aims to enhance regional connectivity infrastructure. Major initiatives under the Act East policy include the India-Myanmar-Thailand Trilateral Highway, Kaladan Multi-modal project etc.

Black Money

7.1. INTRODUCTION

The subject of black money has become a part of everyday public discourse and the ways to bring back black money held in foreign accounts is hotly debated almost every day on news channels. As election approaches political parties allege each other for using black money, black income, unaccounted wealth/economy, illegal wealth to lure the voters. Also, the same black money is the source of funds for criminals and terrorists to carry out various illegal activities.

Despite this, there is no consensus on the official definition of black money. It is defined differently by different agencies of the nation and the globe. Commonly, it is being understood as **the amount on which tax is not paid** or the **amount which is hidden from the tax authorities.** However, this technical definition may not hold true for events such as doing charity, paying money to rickshaw pullers, day to day tasks of small amounts. Difficulty in defining black money also leads to problems in estimating it. The Standing Committee on Finance estimated that the amount of black money may vary from **7% of GDP to 120% of GDP**. This highlights the wide variance in the methods of estimation.

Generally, black money is associated with criminal activities such as drug trafficking, fake currency, organised crimes. However, a series of leaks such as Pandora papers, Panama papers, Paradise papers suggests otherwise. These leaks show that many successful businessmen, renowned actors, and influential political leaders also stash large amounts of money in offshore accounts to evade taxes. These countries/territories/ jurisdictions are known as **tax havens** and have very low or zero taxes.

According to a report released by US based think tank **Global Financial Integrity (GFI) 2020**, India has the **third**-highest trade-related illicit financial flow among more than 135 countries with an amount of USD 83.5 billion followed by China and Mexico. Also, the Swiss government has released data which showed that the amount of funds of Indian individuals rose to 20700 crore (2.55 billion Swiss francs) in 2020. However, the amount of the UK is 377 billion and the USA is 152 billion. Others in top were West Indies, France, Hong Kong, Germany, Singapore. This shows that the concept of black money is not unique to India but also a feature of well-developed advanced economies.

7.2. SOURCES OF BLACK MONEY IN INDIA

Major chunks of black money are generated from illegal means. It includes criminal activities such as bribery, extortion, kidnapping, embezzlement, trafficking, smuggling, poaching, drugs, illegal mining etc. Money earned through these **illegal and corrupt practices** cannot be shown as legitimate income as they fear prosecution by various law enforcement agencies such as anti-corruption bureau, revenue officials, vigilance officers etc. Thus, they try to hide this illegal wealth without paying taxes on it.

Another factor which contributes to generation of black money is various scams due to **political-bureaucrats-businessmen nexus**. They are able to

manipulate spendings on various schemes, public infrastructure and are able to generate a lot of money through these activities. Moreover, amounts involved in scams are very high to the tune of lakhs of crores. This is prominently witnessed in developing countries where poverty and illiteracy is rampant and people at powerful positions often misuse public resources to their advantage. Eg:- In **2G scam**, CAG reported that licenses were issued at throwaway prices even to ineligible applicants causing heavy loss to exchequer and windfall gains to telecom operators. In **commonwealth games** scam as well, substandard assets were created and only half of the allocated amount was spent on the sports person. **Coal gate** scam (coal allocation scam) was also an example of crony capitalism where CAG accused the government of allocating coal blocks in an inefficient manner.

Yet another feature associated with developing countries is the **high rate of taxation**. It has been witnessed that developing countries to meet their needs and take care of the vulnerable population have very high tax rates as high as 30%. Businessmen and high net worth individuals (HNIs) find safer routes to save their wealth from being taken away in form of taxes by the government. This leads to adoption of various tax evading techniques such as round tripping, transfer pricing, base erosion and profit shifting.

In countries like India, one of the most famous ways of stashing black money is in the form of **jewellery, ornaments and bullions**. Gold imported through official as well as unofficial channels (smuggling) is a major way to stash black money. Moreover, the bullion and jewellery market allows the buyer the option of converting black money into gold and bullion, while it gives the trader the option of keeping unaccounted wealth in the form of jewellery, not disclosed in the books of the company.

Experts view **buying and selling of real estate or properties** as another major source of black money generation. State governments fix the **'circle rate'** below which a property transaction cannot be registered. However, the market value of property is usually much higher than the circle rate fixed by the government. So, properties are usually sold/bought at a higher price, but buyers/sellers declare their transaction value closer to the circle rate in order to partially evade taxes such as stamp duty and capital gains tax. Usually, these transactions take place in cash and often, this cash is amassed through unscrupulous means. **Real estate** is also a sink for investing hoarded black money due to **poor titling** (property record maintenance) practices creating ample opportunities for **benami transactions**.

Various taxation laws mainly in the form of direct taxes create confusion. Certain exceptions, privileges are also provided for various sections. They are often used by individuals, businesses, charitable institutions, and non-profitable institutions. Since there are enormous laws which deal with direct taxes, it creates confusion to tax authorities and these loopholes are being used to evade taxes and thereby creating black money in the system. Thus, there is an ongoing demand to codify various direct taxes (DTC) under one regime like GST (for indirect taxes).

In India, there is an **enormous presence of a large informal sector** to the tune of 92 percent which employs more than 80 percent of the workforce and accounts for more than 50 percent of the GDP. Their salaries are paid in the form of cash. Often it is being used to divert black money and show it as payments to workers which can't be ascertained due to contractual nature of work. Further, large amounts of poverty, limited reach of banks to rural hinterland also helps in making cash the most desirable form of transaction. This cash economy is very tough to monitor and remains largely unaccounted for. This leads to generation of black money.

Financial markets related irregularities such as **manipulations in initial public offerings, participatory notes, rigging of markets, insider trading, shell companies** also lead to generation of black money. **Art and artworks** can be used as another source of money laundering or an attractive method to convert black money into legal money. Art works can be hidden for years or even smuggled. Transactions often are private and prices can be subjective, easily manipulated and extremely high. New technologies like **cryptocurrency** and even **NFTs (non-fungible tokens)** have emerged as new methods to launder money and also are used to fund illicit activities without being tracked.

7.3. IMPACTS OF BLACK MONEY

The above methods lead to a vast amount of black money generation. It has various consequences upon different sectors. It has economic, social, political, legal, industrial, and ethical aspects. We shall see them one by one in detail:

The **most affected** due to black money is the **economy**. Generation of black money in an economy leads to development of a **parallel economy**. It leads to functioning of an unsanctioned sector whose interests run opposite to the government. The main issue concerning the parallel economy is **loss of revenue/tax to the exchequer**. It has long term impacts for the government as it may lead to increased borrowings and thereby rise in fiscal deficit in an economy. It generates an interest burden for the future generations.

Moreover, this loss of revenue may be accompanied by inadequate allocation to the **social** sector programmes of the government. This may **negatively impact the vulnerable** and weaker sections of the society. Moreover, the amount which could have been used productively gets diverted to unproductive sectors such as gold, real estate and remains unused. Social impacts of black money may also lead to an increase in inequality in wealth. In India, 1% of the rich hold about 42.5% (2020 report) of the national wealth according to the Oxfam Inequality Report. The social consequence often leads to moral and ethical consequences.

The black money generation also affects the **credibility of commercial sectors** as well. The practices adopted by private companies to evade taxes bring them a bad name when exposed. It thus questions the credibility and people's trust in the private sector gets affected.

As the society witnesses that people with black money are rising in society economically and materialistically, they at times try to emulate them. This gives rise to choosing wrong role models for going up in the ladder. Also, it disincentives honest people who follow legal norms and consider paying taxes their civic duty. It thus becomes a **moral hazard** wherein it creates incentives to take the risk as the individual may not necessarily be held responsible for it. It also sets a **wrong precedent** of following illegal means to become rich and have a luxurious life. The **demonstration effect** it has on youngsters may erode the moral and ethical fabric of the society.

It may fuel organized crimes, drug and narcotics trade, human trafficking and disturb the social harmony. Vast amounts of resources are being used to target and bring back black money into the legal system which could have been used otherwise.

The rise in various forms of crimes can have **security implications** as well. It may also be used by non-state actors to finance criminals and carry out proxy warfare strategies, support sleeper cells, terrorist activities, pump counterfeit currency and destabilise the security and integrity of a country. There have been allegations that black money is being used by separatists agencies to support their causes and hinder developmental processes of the enemy nation. This has been witnessed in **Jammu and Kashmir militancy** (black money from Pakistan). Often, sustenance of Naxalism is also attributed to black money earned from illegal cash collections, bank robbery etc. All these issues may increase the **cost of law-and-order maintenance.** Government would have to invest additional amounts to tackle these issues which could have been otherwise used for other purposes. One of the major objectives of the **demonetisation** was to do away with the black money.

Furthermore, in modern democratic countries, **elections** correspond to spending a large amount of money by politicians and political parties. As per various reports around 55000 to 60000 crores of amount has been spent in the last Lok Sabha election 2019. Various laws allow companies even in loss to fund elections which may lead to creation of shell companies. Foreign funding also allows pumping of black money in the elections. These amounts are used to carry out massive election campaigns, dominate politics, buy votes (cash for votes) and distribute freebies. This also questions the democratic setup of a country as it deprives the poor candidates of a fair chance to win the elections. This denigrates the status of elections which are supposed to be free and fair for all. Moreover, it also questions the credibility of other institutions such as law and order agencies, police, bureaucracy, media, judiciary to implement law in the country.

7.4. MEASURES TO TACKLE BLACK MONEY

It is necessary to adopt measures to tackle this menace since its impacts are wide ranging. Measures adopted must cater to the multidimensional aspect of the issue. Various measures at multi-level needs to be taken to tackle it at various levels such as administrative, legislative etc. A host of measures have been taken which are discussed below under various heads:

7.4.1. Administrative Measures

Central Board of Direct Tax (CBDT) committee has identified the following strategy to tackle black money:-

Preventing generation of black money	India **should** ensure transparent, time-bound & better regulated approvals/ permits, single window delivery of services to the extent possible and speedier judicial processes.
Discouraging use of black money	Government **should** consider amending existing laws (The Coinage Act 2011, The Reserve Bank of India Act 1934, FEMA, IPC, Cr PC, etc.), or enacting a new law, for **regulating the possession and transportation of cash,** particularly putting a limitation on cash holdings for private use and including provisions for confiscation of cash held beyond prescribed limits.
Effective detection of black money	The RBI **should** consider stricter implementation of Know Your Customer (KYC) norms and limit the number of accounts that can be introduced by a single person, the number of accounts that can be maintained in the same branch by any entity and alerts the same address being used for opening accounts in different names. This would lead to effective detection of black money.
Effective investigation and adjudication	Government **should** consider ways to mitigate the manpower shortage issues which are seriously hampering the functioning of various agencies particularly the Central Board of Direct Taxes and Central Board of Indirect Taxes and Customs.

With the **Income Declaration Scheme, 2016**, the government provided an opportunity to those who haven't declared their income properly and allowed citizens to disclose undeclared income with penalty. On 8th November **2016**, the government with an objective to curb the widespread use of high denomination notes for illegal transactions and black money **demonetised Rs500 and Rs1000.** Demonetisation strips the legal validity of a legal tender. It was also aimed to formalise the economy encourage digital economy and boost government tax revenues.

Government to tackle double taxation has come up with Double Taxation Avoidance Agreements (DTAA). However, companies with the adoption of aggressive tax planning measures, business arrangements have misused the loopholes to evade taxes. An incident occurred in 2007 when Vodafone bought the Hutchison Essar and the deal took place in Cayman Islands. The Indian government claimed $2 billion taxes . However Vodafone refused to pay and said that the transaction was not taxable as it was between two foreign firms. The government claimed that the deal was taxable as the underlying assets involved were located in India. However, the Supreme Court ruled in the favour of Vodafone leading to loss of revenue.

To deal with such issues, the government has come out with a set of rules called **General Anti-Avoidance Rules (April 2017)**. It has been framed by the Department of Revenue under the Ministry of Finance. The rules allow tax officials to deny tax benefits, if a deal is done with the sole objective of avoiding taxes and has no commercial purpose. It also allows officials to deny double taxation avoidance benefits, if deals are made in tax havens and are found to be avoiding taxes.

Further, the companies at times define tax havens as their place of residence to evade taxes. To cater to this, Place **of Effective Management' (POEM)** rules **2017** have been formulated. It basically determines the residential place as one where key management and commercial decisions necessary for the conduct of business of an entity as a whole are being taken. Thus, the GAAR and POEM rules out the concept of **treaty shopping** in which the third party takes advantage of the tax treaty between two countries.

One of the measures adopted by various governments across the globe is **use of technology** to keep an eye on generation of dubious transactions mainly related to high value transactions. The Indian government and tax authorities have taken a host of measures to integrate technology as an effective means to counter - generation, storage or continuation of black money in the economy.

Central Board of Direct Taxes (CBDT) has launched **Non-filers Monitoring System** to have focused attention on non- tax filers with potential tax liabilities. The system assimilates and analyses various information as well as transactional data received from third parties to identify persons who had undertaken high value financial transactions but did not file their returns. Similarly,

The Ministry of Finance has launched **Project Insights** to monitor high value transactions and detect tax evaders using technology with a view to curb circulation of black money.

CBDT has also launched Operation Clean Money for e-verification of large cash deposits made during the period of demonetisation. Many series of this operation have been launched since then.

A number of other **measures** taken by the government **to reduce the volume of cash transactions** in the economy and enable its digitisation. Digital transactions create its **digital footprints** and can be traced to its origin easily. Various wallets such as BHIM, UPI are being encouraged and the changes are noticeable. National Payments Corporation of India (NPCI) has launched **Bharat Interface for Money (BHIM)** (a mobile payment app) to facilitate cashless transactions and e-payments. **Unified Payments Interface (UPI)** is a system that powers multiple bank accounts into a single mobile application merging several banking features, merchant payments etc.

7.4.2. Legislative Mechanisms

Parliament has passed various laws to curb generation and circulation of black money in the economy. Often businessmen use various documents under one name to evade the measures adopted by financial institutions. In this backdrop, it has been seen that there have been cases of duplicate PAN cards. PAN card is used to monitor transactions of an individual or a company. When there are multiple pan cards, it becomes difficult to monitor transactions and the transactions can be carried out under pseudo names. In order to **eliminate bogus/multiple permanent account number** (PAN), a new section **139AA** has been inserted in the **Income-Tax Act,** which mandates quoting of Aadhaar number for filing of income tax returns and in PAN application form. Since the Aadhar number is one for one individual, the linkage of Aadhar and PAN will give authorities enough scope to track the digital footprints of an individual.

Yet another measure adopted by the government to strike at the root of black money in day to day life is **Prevention of Corruption Act, 1988. It** has been enacted to consolidate and amend the various laws relating to the prevention of corruption particularly in the government agencies and public sector businesses. However, MPs and MLAs have been kept out of the act. **Amendments** have been made in **2018** to make even "giving bribes" an offence. The amendment has added fraudulent misappropriation of property and illicit amassment of wealth as criminal misconduct.

Also, methods to conceal real income are changing in the modern arena. There have been cases that, a person carries out transactions without using his/her name. Generally, one's own identity is concealed and others identity is used to carry out significant transactions, buy properties etc. This saves such property and persons from being taxed. These transactions are called **benami(property without a name) transactions.** The amount under benami transactions has been rising. Thus **Benami**

transaction act 1988 has been passed to counter it. The act has been **amended in 2016** to define the various forms of benami transactions, liabilities and punishment thereof and also provides for creation of special courts, appellate authority etc.

As we have discussed earlier, one of the main issues which relates to black money generation is the **informal economy** which supports **cash transactions.** Further, there are challenges in an informal economy to make any business compliant with all the rules and regulations and trace the transactions. Too many taxes prompt businesses to go underground and this leads to black money generation. To tackle a lot of such issues and streamline the indirect taxation system of the country, the **Goods and Services Tax Act,2017** has been passed. It will encourage usage of PAN and Aadhar for filing of GST returns. Goods and Services Tax Identification Number (GSTIN)- a unique 15 digit number is assigned to every taxpayer under the GST regime. It will allow income tax authorities to track transactions and call for more data mapping in a more holistic manner. Moreover, the mechanism of **e-way bills** ensures that movement of goods are properly tracked and are in compliance with the GST Law. This checks tax evasion and black money generation in the economy. Thus GST can be said to be a weapon to formalise, digitize and streamline the economy.

Moreover, India has also sought to incorporate international community guidelines in the fight against black money. It has signed and ratified the United Nations Convention Against Corruption **(UNCAC)** in 2011. UNCAC obliges the states to prevent and criminalize different corrupt practices, promote international cooperation, cooperate for the recovery of stolen assets and enhance technical assistance and information exchange. India has also been proactive in building cooperation with countries being viewed as Tax havens and are most probable sources of round tripping the black money. It has thus signed **Tax Information Exchange Agreements** with various countries so as to routinely obtain banking information from countries popularly known as tax havens.

To counter the use of black money, **electoral bonds** have been introduced in India. It is available from Rs 1000 to Rs 1 crore. Since the amount is being paid from account it ensures Know Your Customer(KYC) norms by Reserve Bank of India. It will reduce the anonymous cash donations to political parties. It will also bring transparency in the funding of elections.

7.4.3. Institutional Mechanisms In India

There have been various mechanisms to oversee and implement laws, rules and regulation related to black money in India. The **Central Board of Direct Taxes (CBDT)** under the purview of the Ministry of Finance is a statutory authority functioning under the Central Board of Revenue Act 1963. It provides essential inputs for policy and planning of direct taxes in India, it is also responsible for administration of direct tax laws through its Income Tax arm.

The **Serious Fraud Investigation Office (SFIO)** under the Ministry of Corporate Affairs takes up investigation of complex cases having inter-departmental and multidisciplinary ramifications and substantial involvement of public interest. It also takes up cases where investigation has the potential of contributing towards a clear improvement in systems, laws, or procedures. **CERT-FIN** (Computer Emergency Response Team for Financial sector) has been established as per Information & Technology Act. It will work with all the financial regulators and mainly deal with the cases of cyber security. Its need was felt due to increasing instances of cyber frauds committed due to increased digitalisation of the economy.

The **Economic Intelligence Council (EIC)** chaired by the Finance Minister takes decisions regarding trends in economic offences and strategies on intelligence sharing, coordination, etc. **Central Economic Intelligence Bureau (CEIB)** functioning under the Ministry of Finance is responsible for coordination, intelligence sharing, and investigations at national as well as regional levels amongst various law enforcement agencies.

Central Vigilance Commission (CVC) was established in 1964 but the Central Vigilance Commission (CVC) Act 2003 gave statutory status to CVC. As the apex integrity institution, the Commission is mandated to fight corruption and to ensure integrity in public administration.

7.5. WAY FORWARD

Although India has taken a number of measures to tackle this menace, various other steps need to be adopted to strike at the very root cause of generation of black money. It has to be taken into consideration that often the generation of black money and money laundering is an interrelated process, the measures adopted to tackle any one of the two has a bearing on another and thus are overlapping in nature.

The first measures which can augment the existing steps taken by the government is targeting the various factors which contribute to generation of black money. Complicated tax structure and high rate of taxation creates incentive for tax evasion. Voluntary compliance can be ensured by rationalization of tax rates and simplifying online tax filing procedures. **Slashing of corporate taxes** from 30% to 22% for existing companies and 15% from 25% for new manufacturing companies are steps in a positive direction.

Sectors vulnerable to generation of black money such as **real estate and gold** must be strictly regulated. Wherever possible, duties and taxes such as stamp duties, properties taxes can be rationalised. Focus should also be on making economy- digital economy so that the existing loopholes which lead to cash transactions can be checked. Use of credit, debit cards, UPI payments, digital wallets can be incentivised as a measure.

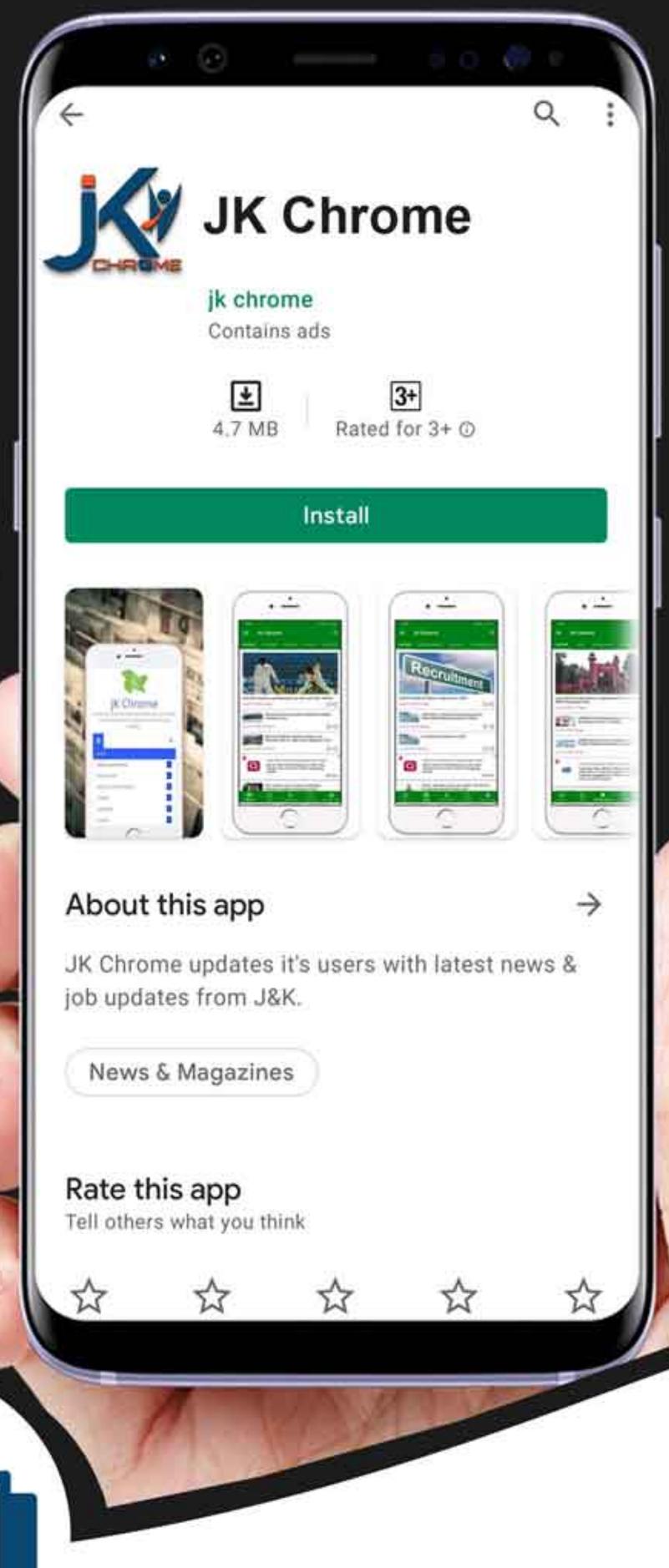
Policies should create enough disincentives for black money generation. Creation of effective credible deterrence to the tune of disincentivizing generation of black money must be kept in place. The **introduction of GST** is an important step in this process. Encouragement to strengthen direct tax administration, prosecution mechanisms must be put in place for proper implementation of policies. Further, exchange of information must be enhanced between various stakeholders. This needs to be emulated for bringing in direct tax reforms as well.

The root cause which presently dominates black money generation, and its use is lack of transparency in funding of elections. The voting at Vellore was cancelled in 2019 Lok Sabha by President after Election Commission's recommendation when around 12 crores in cash was seized. Thus, the government needs to attack use of black money during elections by making electoral funding transparent, curbing the misuse by the politicians of tax-free income sops for farmers, and encouraging cashless transactions. **State funding of elections** as suggested by committees such as **Indrajit Gupta Committee (1998)** can be a way forward.

Further, the Indian economy is largely informal in nature and is cash driven. Efforts must be taken to move towards formalisation of economy or promotion of digital economy which can minimize various loopholes of the economy. The channel of **Direct Benefit Transfer** can be used to transfer the subsidies to various stakeholders of the economy. It reduces corruption in public administration and the targeting of schemes also becomes better. Further, digital transactions are easier to monitor than the cash. Supportive measures such as creating **public awareness** and public support, enhancing the **accountability of auditors** and participating in international efforts are recommended.

JK Chrome

JK Chrome | Employment Portal



Rated No.1 Job Application of India

Sarkari Naukri
Private Jobs
Employment News
Study Material
Notifications

JOBS

NOTIFICATIONS

G.K

STUDY MATERIAL

GET IT ON Google play

JK Chrome
jk chrome
Contains ads

Click here to DOWNLOAD

www.jkchrome.com | Email : contact@jkchrome.com

Money Laundering

8.1. INTRODUTION

In general terms, money laundering can be understood as a process by which black money is converted into white money. In doing so, the origin of the **black money** is **concealed** and it is pumped back into the economy. According to **INTERPOL**, Money laundering is concealing or disguising the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. Some of the common methods of money laundering are bulk cash smuggling, shell companies and trusts, round-tripping, hawala, false invoicing etc. Though it is done to mostly evade taxes and disguise money's origination point, it is also frequently associated with terrorist funding, arms trafficking and other organized crime at national and global level. The advent of cryptocurrency such as bitcoins has exacerbated this phenomenon.

8.2. PROCESS OF MONEY LAUNDERING

Often, money laundering is considered a single process. However, its cycle can be broken down into three distinct stages namely, placement stage, layering stage and integration stage.

Placement Stage is the stage at which illicit funds are introduced into the financial system. At this stage, the launderer inserts the "dirty" money

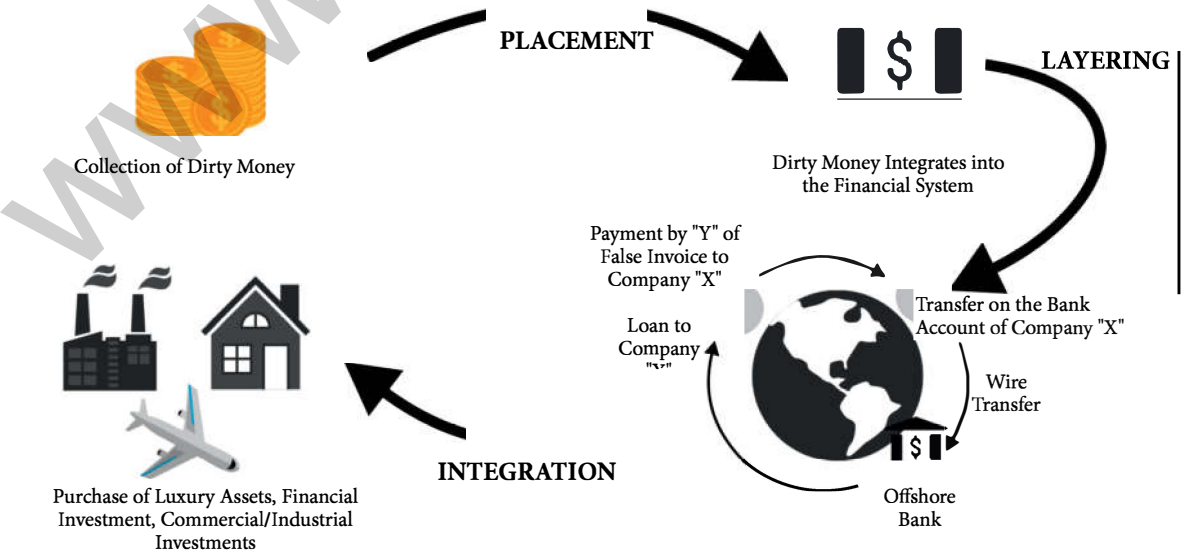


Figure 8.1: *Process of Money laundering*

into a legitimate financial institution mainly in the form of cash deposits. Here, the large amount of cash is broken into smaller sums and deposited into different bank accounts. The launderer may also buy precious goods such as gold, diamond, artworks which can be further resold, the proceeds of which can be received by bank transfer. This is the riskiest stage of the laundering process because large amounts of cash are pretty conspicuous, and banks are required to report high-value transactions. Eg: Cash-intensive businesses - In this method, a business typically receives a large proportion of its revenue as cash and uses its accounts to deposit illicit cash.

The second stage is the **layering stage** in which **complex financial transactions** are carried out in order to hide the illegal source. At this stage, the launderer through a **series of conversions** with the help of multiple financial intermediaries such as banks situated across the **globe** changes the **form of money** through various financial transactions so that it becomes difficult to follow. This is often done by changing the money's currency, carrying out **multiple interbank transfers,** investing in stocks and bonds. Eg: the launderer might simply channel the funds through a series of accounts at various banks across the globe.

The final stage is **integration** in which the illegality of the laundered amount is concealed and is reintroduced into the **mainstream financial system** as legitimate. At this stage, the launderer may choose to invest the funds into real estate, luxury assets or business ventures. This is being achieved by **using front companies and taking false loans, issuing false export invoices** etc. It's very difficult to catch a launderer during the integration stage if there is no documentation during the previous stages. Eg: **Round-tripping** - Here, money is first deposited in a foreign corporation offshore preferably in a tax haven where minimal records are kept. They are then brought back to the original country as foreign direct investment in the original country's economy.

8.3. METHODS FOR MONEY LAUNDERING

Various mechanisms are used to launder money. It can be in the form of **structural deposits** also known as **smurfing**. This is a method of placement whereby cash is broken into smaller chunks of money and is deposited into various bank accounts. This does away with suspicion and avoids anti-money laundering reporting requirements as required by financial institutions and various agencies of the government for transactions beyond a certain threshold.

Another common way to launder money is by the creation of **shell companies.** Shell companies are those companies which do not have any active business operations or significant assets. Organization for Economic Co-operation and Development (OECD) defines shell companies as **a firm that is formally registered, incorporated, or otherwise legally organized in an economy but which does not conduct any operations in that economy other than in a pass-through capacity**. Shell companies are incorporated primarily to conceal the assets of their owners. It facilitates tax evasion, prevention from legal indictments and money laundering. They take in black money as 'payment' for a particular goods or services but actually provide no goods or services. Thus, they simply create the appearance of legitimate transactions through fake invoices and balance sheets. Third-party cheques, banker's drafts drawn on different institutions are utilized and cleared via various third-party accounts. These cheques and drafts are often purchased using proceeds of crime. Since these are negotiable in many countries, the nexus with the source of money is difficult to establish.

Bulk cash smuggling is another frequently used method to launder money. In this process, a bulk amount of cash is physically smuggled to another jurisdiction. There, they are deposited in financial institutions, such as an offshore bank. These places generally have greater bank secrecy or less rigorous enforcement of anti-money laundering laws.

Hawala Transactions as opposed to bulk cash smuggling works by transferring money without any physical movement of cash with the help of brokers. It is an alternative or parallel remittance system, which works outside the domain of banks and formal financial systems. Since these transactions are not routed through banks, they cannot be regulated by the government agencies. Hawala in common usage means trust. The hawala

system works with a network of operators called Hawaladars/Hawala Dealers/Brokers. A person willing to transfer money, contacts a **'hawala operator'** at the source location who takes money from that person. The hawala operator then calls upon its counterpart at the destination who gives the cash to the person to whom the transfer has to be made, thus completing the transaction.

Hawala is illegal in India, as it is a form of money laundering. Since hawala transactions are not routed through any financial institutions, government agencies and the Reserve Bank of India cannot regulate them. In India, **Foreign Exchange Management Act (FEMA) 2000 and Prevention of Money Laundering Act (PMLA), 2002** are the two major legislations which make such transactions illegal. (These are discussed later in this chapter)

Hawala as a route to launder money is gaining increasing popularity due to several factors. The commission rates charged for transferring money through hawala are quite low. There is no requirement of any identity proof or disclosure of source of income as required in financial institutions such as banks. Moreover, the Indian rupee is still not fully convertible and cannot be exchanged beyond a prescribed limit, money transfer through hawala circumscribes this restriction. Hawala provides an easier and cheaper alternative for conversion of Indian currency to foreign currency. Money transfers made through Hawala are free from strict scrutiny of FEMA Act. Thus, the hawala system being cheaper, faster and opaque fulfills all the requirements of launderers. Thus, it has emerged as a major cause of concern and is frequently used by criminals to launder money for their illicit acts. Hawala network is being extensively used across the globe to circulate black money and to provide funds for terrorism, drug trafficking and other illegal activities.

8.4. IMPACT OF MONEY LAUNDERING

Money laundering directly affects the **economy** of a country as it **undermines the integrity of financial markets** and its regulators. Money laundering dampens foreign investment as it may force investors to invest in economies that are perceived to be less exposed to the risk of money laundering. It also **undermines the legitimacy of the private sector** by bringing a bad name to it. Use of front companies by money launderers questions the credibility of the legitimate private sector. It leads to **economic distortion and instability.** Further, it may also misrepresent capital flows, and thus destabilise the effective functioning of the world-wide economy.

It has a vast macroeconomic effect and leads to **volatility in exchange rates and interest rates** due to unanticipated transfers of funds. It also leads to rise in commodity prices, the effect of which is felt by underprivileged sections. It also impacts the **external sector.** Excessive illegal capital movement from a state may be facilitated by domestic financial institutions such as banks with the help of P-notes. Participatory notes or PNs or P- notes were the financial instruments used by the investors to invest in the Indian market without registering with the Security and Exchange Board of India. Moreover, at times big businessmen are able to get huge amounts of loans by **fabricating their collateral to be of high value or banks find themselves without collateral in case of various frauds** involving defaults by the parties concerned. They often take Indian money and deposit it in offshore banks working as safe havens. This illicit capital flight drains scarce resources, especially from developing economies. In this way, economic growth of a developing country is adversely affected.

The main economic impact of money laundering is that it leads to **loss of revenue to the public exchequer. This, in a way restricts the fiscal cushion available with the government which could have been used for social sector** schemes aimed at uplifting lower strata of the society, in a country like India. It also has other social **externalities.** It may lead to **increased criminality in society** as the triumph of money launderers and their lavish lifestyles may lead to misguided youth emulating them. It can also affect trust of local citizens in the government and domestic financial institutions if they are not able to curb money laundering activities. It can also have **debilitating impact on moral and social position** of the society and expose them to activities such as **drug trafficking, smuggling, corruption** etc.

Political Impacts of money laundering includes **decline of social trust** of politicians among local population as they are not capable to tackle money laundering activities. Moreover, the entry of laundered money into the election process leads to **criminalization of politics** and absence of level playing field.

National Investigation Agency (NIA) investigations on terror funding in the Kashmir valley have revealed that the separatist groups in Kashmir have been receiving a steady flow of funds through the 'hawala' route through Pakistan and UAE-based businessmen. The cases of terror funding are registered in general under Sections 120-B (criminal conspiracy), 121 (waging war against government) of IPC and Sec 17 of Unlawful Activities (Prevention) Act, 1967 (terror financing) and Prevention of Money Laundering Act (PMLA), 2002.

8.5. COMBATING MONEY LAUNDERING

Various legislative measures have been taken in order to curb the menace of money laundering. It is covered under various laws as the issue can arise out of many multiple dimensions -

In order to curb the money laundering arising out of bribes, breach of trust and cheating, **Criminal Law Amendment Ordinance (XXXVIII of 1944)** has been brought in. Under it, actions can be taken upon the employees of the central as well as the state government. Authorities can forfeit the proceeds of crime relating to these offences and also confiscate it on the orders of the court.

Since the process of money laundering is related with transboundary operations and often involves activities of smuggling, **The Smugglers and Foreign Exchange Manipulators (Forfeiture of Property) Act, 1976** has been passed which provides for penalties in case of illegally acquired properties by smugglers and foreign exchange manipulators. However, the application of this law is restricted to persons convicted under the Customs Act, 1962 or Sea Customs Act, 1878 or other foreign exchange laws.

Of late, it has been seen that black money is being diverted for buying drugs through various peddlers and these are finding increased penetration among urban youths. To deal with such cases, **Narcotic Drugs and Psychotropic Substances Act, 1985 has** been passed which provides for the **forfeiture of property** derived from illegal trafficking of narcotic drugs and psychotropic substances.

Prevention of Money-Laundering Act, 2002 (PMLA) forms the core of the legal framework put in place by India to combat money laundering. It identifies certain offences under various laws such as Indian Penal Code, Narcotic Drugs and Psychotropic Substances Act, Arms Act, Wild Life (Protection) Act, Immoral Traffic (Prevention) Act and Prevention of Corruption Act, the proceeds of which can be covered under this Act. It also tackles cross border money laundering activities. It further allows the central government to enter into an agreement with other countries for enforcing the provisions and exchange information for the prevention of offences under PMLA.

It has provisions for the establishment of **special courts** which have been set-up in a number of States / UTs by the central government to conduct the trial of the offences related to money laundering. The act has brought financial institutions like Full Fledged Money Changers (FFMC), Money Transfer Service and Master Card within the reporting regime of the act. The Act also prescribes for formation of a three-member **adjudicating authority,** one each from the fields of **'Law', 'Administration' and 'Finance or Accountancy'.** It functions within the Department of Revenue; M/o Finance of the Central Government with its headquarter at New Delhi. An **Appellate Tribunal** is established to hear appeals against the orders of the adjudicating authority and the authorities under the Act.

8.6. CHANGES IN THE PMLA, 2002 THROUGH FINANCE ACT, 2019

Amendments in the **Prevention of Money Laundering Act** have been brought in with an aim of enhancing the effectiveness, widen its scope and remove procedural difficulties faced by the Enforcement Directorate (ED) in prosecution of PMLA cases. This has been done through bringing in changes such as making money laundering a stand-alone crime. Earlier, various provisions which required FIR or charge sheet to be filed by the other agencies have been done away with.

Further the crime under PMLA has been **explicitly stated to be cognizable and non-bailable.** This will empower ED to arrest an accused without a warrant, subject to certain conditions.

The **definition of proceeds of crime** in PMLA has been amended to expand its meaning. The present amendment shall allow to proceed against assets that may have been derived from any other criminal activity related to scheduled offences. It includes the proceeds held outside the country as well. **Corporate frauds have been included as scheduled offences**. Section 447 of the Companies Act is being included as scheduled offence under PMLA so that the Registrar of Companies in suitable cases would be able to report such cases for action by the Enforcement Directorate under PMLA. This provision shall strengthen the PMLA with respect to corporate frauds.

There has been amendment in bail provisions in Section 45(1) that would make the **applicability of bail conditions uniform to all the offences** under PMLA instead of only those offences under the schedule which were liable for imprisonment of more than 3 years. Also, the jurisdiction of special courts dealing under this act shall not be dependent upon any orders passed in respect of the scheduled offences. This means to say that the **trial of offences will not be considered as a joint trial**. This will be a significant step forward in delinking the proceedings against scheduled offences and Money laundering offences under PMLA.

Measures have been taken for restoration of property of persons adversely affected by PMLA investigation. Present provisions under Section 8(8) allowed distribution of confiscated property to the rightful claimants, only after the completion of the trial. Present amendment allows the Special Court to consider the claims of the claimants for the purposes of restoration of such properties even during the trial.

The Fugitive Economic Offenders Act, 2018 has been promulgated to confiscate properties and assets of economic offenders who evade prosecution by remaining outside the jurisdiction of Indian courts. **Fugitive Economic Offender is a person against whom an arrest warrant has been issued for committing an offence listed in the Act and the value of the offence is at least Rs. 100 crore.** It includes offences related to money laundering, cheque dishonour, counterfeiting governments stamps or currency etc.

India has also become signatory to various intergovernmental agreements such as **The Foreign Account Tax Compliance Act (FATCA).** FATCA is a USA federal law that requires US citizens to report their financial accounts held outside USA. It also requires reporting from foreign financial Institutions and certain other non-financial foreign entities. The reporting is on the foreign assets held by U.S. account holders in Indian institutions.

Recently, India has also **amended its Double Taxation Avoidance Agreement (DTAA) with Mauritius.** Mauritius will now provide for source-based taxation of capital gains on shares and income of banks. This has been done as it was seen that vast amounts of funds were brought back by misusing this agreement by a process called round tripping. Moreover, various companies have employed aggressive tax avoidance methods with tools of **treaty shopping**. The **India Singapore Double Taxation Avoidance Agreement (DTAA) was also amended** to provide for source-based taxation of capital gains on shares, to enable measures concerning prevention of tax evasion and tax avoidance.

Moreover, larger companies using the double taxation avoidance agreement and aggressive tax planning methods carry out deals in tax havens to evade taxes although their assets lie in some other countries. Thus, these deals have no other commercial interests but to avoid taxes. This has been witnessed in India in the famous Vodafone case where **Vodafone ventured into the Indian market by buying Hutchison Essar.** The deal was carried out in the **Cayman Islands having no commercial relevance**. The Indian government suffered loss to the tune of 2 billion and the supreme court gave judgement in favour of Vodafone. To deal with such issues, the **General Anti Avoidance Rule was brought in from 1st April 2017**. It is applicable only if the **benefit arising out of it is 3 crore or more**. This rule gives power to tax authorities to venture into the real intention of the parties to carry out a deal and then determine tax benefits. However, various safeguards are being given so that the rules are not misused by tax authorities.

Double Taxation Avoidance Agreements (DTAA) in the form of a tax treaty is a measure to avoid taxing the same income more than once in different countries.

Round tripping is a process by which the black money taken from a country to another is brought back to the origin country, but now it has taken form of being legitimate money.

Treaty shopping is a method in which a person or a company non-resident in any of the countries takes advantage of a tax treaty (mainly DTAA) between the two governments.

8.7. INSTITUTIONAL FRAMEWORK FOR DEALING WITH MONEY LAUNDERING

The **Directorate of Enforcement(ED)** was established in 1956. It is responsible for enforcement, investigation and prosecution of the cases under Foreign Exchange Management Act, 1999 (FEMA) and certain provisions under the Prevention of Money Laundering Act. Its functions include dissemination of intelligence related to the violation of FEMA, hawala rackets, non-repatriation of foreign exchange.

Prevention of Money Laundering Act (PMLA),2002 also **requires every banking company** to furnish details of **suspicious transactions** whether or not made in cash. It helps to get hold of transactions which have no economic rationale or have reasonable grounds of suspicion that it may involve the proceeds of crime.

Financial Intelligence Unit – India was set by the Government of India in **2004** as the central national agency tasked to process, analyse and disseminate information related to suspected financial transactions. It 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. It is an independent body and reports directly to the Economic Intelligence Council (EIC) headed by the Finance minister.

8.8. GLOBAL EFFORTS TO COMBAT MONEY LAUNDERING

Money laundering as a menace has cross border implications and also involves non-state actors. Thus, efforts have been taken at global level to synergize the efforts of individual countries and provide them with enough capability to deal with this complex issue.

The first major initiative which was adopted for prevention of money laundering was in the form of **The Vienna Convention(1988).** It laid down the groundwork for efforts to combat money laundering activities by obliging the member states to criminalize laundering of money from drug trafficking. The second initiative came when **the Basel Committee on Banking Regulations and Supervisory Practices** issued a statement of principles in **1988.** It encouraged the banking sector to adopt a common set of principles to ensure that banks are not used to hide or launder funds acquired through criminal activities.

However, presently the most important organization which deals with various components of money laundering is **The Financial Action Task Force (FATF).** It is an inter-governmental body established at the G7 summit in Paris in **1989**. Its objective is to set standards and promote effective implementation of legal, regulatory and operational measures to combat money laundering, terrorist financing and other threats to the integrity of the international financial system. FATF has two kinds of lists: **grey list and black list**. Countries which are considered safe haven for supporting terror funding and money laundering are put in the FATF grey list. It serves as a warning to the country that it may enter the blacklist and involves increased monitoring. **Pakistan is presently under grey list since 2018 and Jordan, Mali and Turkey were recent additions in 2021.** Other countries which support terror funding and money laundering activities and do not take corrective measures to stop it are known as Non-Cooperative Countries or Territories (NCCTs). They are put in the blacklist. **North Korea and Iran** are presently under the **blacklist**. The FATF revises the blacklist regularly, adding or deleting entries.

Moreover, there are various regional groupings such as **Eurasian Group** on Combating Money Laundering and Financing of Terrorism (EAG) and Asia **Pacific Group** on Money Laundering (1995) which are also **associate members of FATF** work on the lines of FATF to facilitate the adoption, implementation and enforcement of internationally accepted anti-money laundering and anti-terrorist financing standards set out by FATF. Some organisations such as African Development Bank, Asian Development Bank, Organisation of Economic Cooperation and Development, Interpol are also associated with FATF as observers.

The **United Nations** has also adopted a series of measures to stop the terror financing and activities of money laundering. The UN Global Programme against Money Laundering (1997) is a research and assistance project within the United Nations Office for Drug Control and Crime Prevention **(UNODCCP).** Its main areas of activity include promoting cooperation in training, institution-building and raising awareness, research and analysis on understanding the money laundering phenomenon and raising the effectiveness of law enforcement agencies.

8.9. CHALLENGES IN PREVENTION OF MONEY LAUNDERING

Although efforts have been taken and collaboration at various national and international agencies continues, there have been various challenges in tackling the menace of money laundering. The main framework which allows and sustains it is the **existence of tax havens**. They have been associated with money laundering because their strict financial secrecy laws allow the creation of anonymous accounts while prohibiting the disclosure of financial information. Furthermore, there is strong evidence indicating that a substantial portion of these funds has been used to sustain terrorist groups such as Al-Qaeda.

The poor and illiterate people often lack awareness about the seriousness of the crime of money laundering; instead of going through lengthy paperwork transactions in banks, they prefer the Hawala system where there are fewer formalities, little or no documentation, lower rates and anonymity. Sometimes, there is leniency from the part of the financial institutions due to increasing competition in the market. Thus, often banks are forced to lower their guards and this facilitates the money launderers to make illicit use of it in furtherance of their crime. This at times leads to non-fulfilment of the purpose of Know Your Customer (KYC) Norms.

Moreover, there is a **lack of cohesive and comprehensive efforts between various enforcement agencies**. Separate wings of law enforcement agencies dealing with money laundering, cyber-crimes, terrorist crimes, economic offences, etc. lack convergence among themselves. It gets further complicated to handle when there exists a number of **black-market channels for** the purpose of selling goods. They offer many imported consumer goods such as food items, electronics etc. which are routinely sold. This in a way incentivises smuggling cases.

There have been **rapid advancements in digital technology** which our enforcement agencies are not able to match up. With the speed of growing technologies, money launderers are able to conceal the origin of proceeds of crimes by using cyber finance techniques. Thus the technology needs proactive proper upgradation in concurrence with the modern era.

Furthermore, it has been observed that the best institutions to tackle money laundering such as **Enforcement Directorate (ED) are increasingly being used at the behest of the government in power to settle political scores, gain political mileage and intimidate political opponents. Moreover,** the agency is selectively used to target certain individuals which do not come under the other agencies domain. This undermines the neutrality and reputation of such an agency to fight money laundering activities.

8.10. WAY FORWARD

Special cell dealing with money laundering activities should be created exclusively dealing with research and development of anti money laundering(AML). This special cell should have links with INTERPOL and other international organizations dealing with AML. All key

stakeholders, like, RBI, SEBI etc. should be a part of this.

Implement FATF Recommendations which sets out a comprehensive and consistent framework. Some of them include identifying the risks, developing policies and domestic coordination to mitigate money laundering and terrorist financing risks. Moreover, **FATF's recent guidance** on how financial intelligence units (FIUs)can **leverage technology to strengthen their operations, registering and licensing of virtual assets in a country and encouraging cross border payments** must be taken into consideration to fight emerging challenges in money laundering.

Countries should criminalise money laundering on the basis of the international rules and conventions such as United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (the Vienna Convention) and the United Nations Convention against Transnational Organized Crime, 2000 (the Palermo Convention). This will ensure that the financial institution secrecy laws do not inhibit the implementation of FATF recommendations.

Mutual legal assistance should be provided for between countries so as to effectively execute extradition requests in relation to various crimes of money laundering and terrorist financing. In accordance with this, India has signed mutual legal assistance treaties (MLATs) with 42 countries such as the **United Kingdom, Mexico, Canada, Thailand, Singapore** etc.

The existing laws and regulations related to **non-profit organisations** being vulnerable to terrorist financing abuse should be reviewed. It has been seen that various NGOs are being used as a tool to launder money and create hindrance in the developmental works in the country. The **Enforcement Directorate** had recently attached properties of **Rs 17.66 crore of Amnesty International in violation of Foreign Contribution Regulation Act**. India to overcome this has prescribed a separate report named **Not for Profit Transaction Report** mandatory to be filed by Non-Profit Organisations involving receipts of more than ten lakh rupees.

Thus, there is an increasing need to draw a line between financial confidentiality rules in certain countries and these institutions becoming money laundering havens. This will help in **tackling the menace of tax havens.** There should be continuous up-gradation and dissemination of information so that if there is any aberration from the normal, it can be flagged within time. **The SHERLOC knowledge** management portal facilitates the dissemination of information related to and provides knowledge regarding Anti-Money Laundering and Counter terrorist financing.

Q1. Discuss how emerging technologies and globalization contribute to money laundering. Elaborate measures to tackle the problem of money laundering both at national and international levels. **(UPSC 2021)**

Q2. Money laundering poses a serious security threat to a country's economic sovereignty. What is its significance for India and what steps are required to be taken to control this menace? **(UPSC 2013)**

Cyber Security

9.1. INTRODUCTION

Cyber security includes the techniques of protecting computers, networks, programs and data from unauthorized access or attacks, damage, misuse and economic espionage.

9.1.1. Elements of Cyber Security

There are various elements of securing the cyberspace and its devices. The foremost of which is **application security,** which is the use of the software or hardware to protect applications from external threats. For example, anti-virus software. Secondly it includes **Information security** which is a set of strategies for managing the processes, tools and policies for securing digital information, for example, data encryption software and tools. Thirdly there is **network security,** which entails protecting networks against internal and external threats. For example, Windows firewall in computers protect external threats from entering the computer. Next it includes **disaster recovery plan,** which is a structured plan that guides the response to unplanned incidents. It enables an organisation to resume critical functions. For example, IBM's cloud for disaster recovery. Another aspect of cyber security is **operational security,** an analytical process that classifies information assets and determines controls required to protect these assets. For example, Captcha code. Finally, there is the important element of **end user education,** by making policies to guide users for secure use of an organisation's systems. For example, Google's digital literacy campaign.

Cyberspace and Internet

Internet is a **system of inter-connected devices** using standardized communication protocols. It is a global network created by linking smaller networks of computers and servers, which allows users to share information and other data from one point to another. It can be said that anything that is done via the use of internet, occurs within the confines of the Cyberspace, whether that is sending an e-mail, opening a website, or playing a game. **Cyberspace** therefore, is a complex, abstract and **virtual environment** consisting of interactions between people, software and services, supported by the internet and network devices. Interconnectedness of the cyberspace, multiple internet entry points and dependency of critical infrastructure on the cyberspace makes it vulnerable to cyber threats.

9.2. WHAT IS A CYBER-THREAT?

As per the American political scientist Joseph Nye, there are four primary threats to cyberspace. They include firstly the threat of **cyber espionage,** which is the use of computer networks to gain illegal access to confidential information, typically that is held by a government or other organizations. It is the act of obtaining secret information from individuals, competitors, rivals, groups, governments and enemies, without the permission of the holder of the information, which can be personal, sensitive, proprietary or of classified nature. Information is obtained for personal,

economic, political or military advantage, through the use of code cracking techniques and malicious software including Trojan horses and spyware. For instance, **Pioneer Kitten** is an Iran based hacking group, with close ties to the Iranian government. It has been accused of selling access to compromised foreign government networks on Dark Net. Another group **Fancy Bear**, is a Russia based cyber attacker that has targeted US political organizations and European military organizations over the years. Secondly it includes the threat of **Cyber-crime/ attack,** which is "any type of offensive manoeuvre employed by individuals or whole organizations, to target computer information systems, infrastructures or computer networks, with an intention to damage or destroy a specific computer network or system." For example, hacking of the system and stealing the private data of any user. In 2016, when 32 lakh SBI ATM cards got hacked, it was one of the largest cybersecurity breaches in India's banking system. Thirdly there is the threat of **Cyber terrorism** as the convergence of terrorism and cyber space, which involves politically motivated use of computers and IT to cause severe disruption or widespread fear in society. It includes activities such as websites spreading extremist propaganda, recruiting terrorists, promoting the propaganda of terrorists etc. To qualify as cyber terrorism, an attack should result in violence against persons or property or at least cause enough harm to generate fear. Serious attacks against critical infrastructures could be acts of cyber terrorism depending upon their impact. Finally, **Cyber warfare** includes the actions by a nation-state or its proxies to penetrate another nation's computers or networks for the purposes of espionage, causing damage or disruption. For instance, in 2010, Stuxnet, a malicious computer worm, was designed to attack industrial programmable logic controllers of the Iranian nuclear programme. As an alternative to conventional wars, countries can now resort to such cyberwarfare practices against their rival countries which can disrupt network services and will compromise data of the users.

9.2.1. Types of Cyber-Attacks

There are different forms of cyber-attacks such as, a computer **virus,** which is a program code that attaches itself to application program and when application program runs, it runs along with it. It typically has a detrimental effect, such as corrupting the system or destroying data. Then there is **Malware,** it is a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or otherwise annoying or disrupting the victim. Next there is **Denial of service (DoS),** which is a technology-driven attack that occurs when an attacker prevents legitimate users from accessing specific computer systems and networks. In other words, it is an attack that prevents or impairs the authorized use of information system resources or services. These attacks are used to overwhelm the targeted websites. Attacks are aimed at denying authorized person's access to a computer or computer network. Another form of cyber-attack is **Logic bomb,** it is a computer program, which may perform some useful function, but it also contains a hidden code which, when activated, may destroy data, reformat a hard disk or randomly insert garbage into data files. **Spoofing** as a form of cyber-attack has the ability to fool a biometric sensor into recognizing an illegitimate user as a legitimate user (verification) or into missing an identification of someone who is in the database. Then there is the cyber-attack in the form of **Bluetooth hijacking,** which is an attack conducted on Bluetooth-enabled mobile devices, such as cellular telephones, smart phones, etc. Here the private information is stolen from some other device through Bluetooth without the knowledge of the owner of the device. **E-Mail related crimes** are defined as a cyber-attacks as it aids worms and viruses in attaching themselves to a host programme, for example emails, in order to be injected. E-mails are also used for spreading misinformation, threats and defamatory stuff. Cyber criminals use innovative social engineering techniques like spam, phishing and social networking sites to steal sensitive user information to conduct various crimes, ranging from abuse to financial frauds to cyber espionage. **Phishing** is a cybercrime in which targets are lured by mails to provide sensitive information (personal information, bank details etc.) by someone posing as a legitimate website. For example, Nigerian money transfer scams with emails asking bank account information to transfer

money for safe-keeping, tempting users by emails of winning lottery or some lucky draw, etc. **Spams** are unsolicited commercial emails (UCE) sent to numerous addresses or newsgroups, which may fool a person to pay money or provide information to the wrongdoers. Next form of cyber-attacks are **Spyware,** which are technologies deployed without appropriate user consent and/or implemented in ways that send away the information about user activity without his/her acknowledgement. For example- **Pegasus** spyware, that was in news in 2021, over its ability to stealthily enter a smartphone and gain access to everything on it, including the camera and microphone. Botnet (a contraction of the term "RoBOTNETwork") as a form of cyber-attack is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks like-distribute malware, DoS attacks, steal data, send spam mails, and phishing scams etc. It is a network of compromised computers that are remotely controlled by malicious agents. For example- Mirai Botnet. **Identity theft,** as a cyber-attack includes obtaining and unlawfully possessing identity information of someone with the intent to use the information deceptively, dishonestly or fraudulently in the commission of a crime. As a cyber-attack form **hacking** is a popular method used by a terrorist. It is a generic term used for any kind of unauthorized access to a computer or a network of computers. Some ingredient technologies like packet sniffing, password cracking and buffer outflow facilitate hacking, identity theft, etc. **Trojan** are cyber-attacks in form of programmes which pretend to do one thing while actually they are meant for doing something different. A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. They can be employed by cyber-thieves and hackers trying to gain access to users' systems. Examples of Trojan include the Swiss MiniPanzer and MegaPanzer and the German "state Trojan" nicknamed R2D2. Then there is cyber-attack of **Keyboard logging,** which is a software that captures and "logs" every keystroke typed on a particular keyboard. Finally there is **Pharming,** which is a more sophisticated level cyberattack as compared to **Phishing** but at **DNS level** in which the users are deceived into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed web site when the user types a legitimate web address.

Q1. Discuss the potential threats of Cyber-attack and the security framework to prevent it. **(UPSC 2017)**

Q2. Discuss different types of cybercrimes and measures required to be taken to fight the menace. **(UPSC 2020)**

9.2.2. Steps in Cyber-Attacks

Cyber attacks involve a series of precisely calculated steps to infiltrate a system and create havoc. The first step involves chartering out the motive of the attack, which can range from simple destruction of system, data and processes,

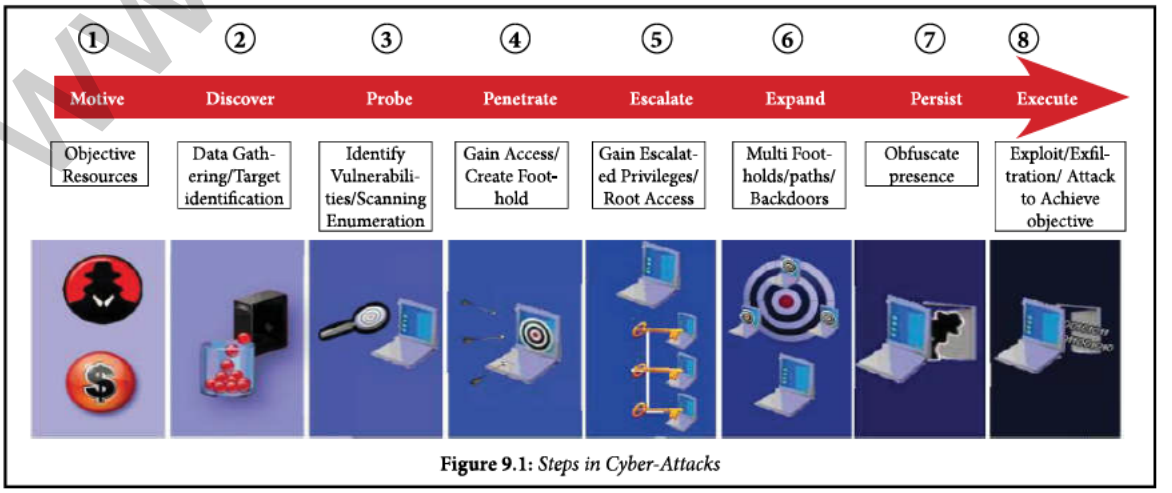


Figure 9.1: *Steps in Cyber-Attacks*

to observing, archival and manipulation of the system, data and processes. The next steps include identification of the target, collection of data regarding the target and identification of vulnerabilities in the system to plan an entry route. Once the access route is established, the attacker penetrates the system, lodges itself into the host network, stealthily, in order to remain undetected. It then tries to gain root access or master key access, so that it can get permission to run any command on the system. Further, the attacker expands its foothold in the host system and creates multiple backdoors for entry and exit of more bugs into and out of the system. The last and the final step is the execution of the planned objective and achieving its mission.

9.2.3. Recent Cyber-Attacks in India

Union Bank of India heist in July 2016 which was conducted through a phishing email sent to an employee was a major cyber-attack. Hackers were able to access the credentials to execute a fund transfer of 171 million Dollars. However, prompt action helped the bank recover almost the entire amount. In May 2017 there was a cyber-attack in the form of **Wannacry ransomware,** in which ransom of money was asked when the computer was locked without the owner's permission and in return for providing access of data back to the owner of the device, once the money transfer is done. The top 5 cities impacted by the ransomware attack were: Kolkata, Delhi, Bhubaneswar, Pune, Mumbai. It also infected the Gujarat State Wide Area Network, computer systems of at least 18 Andhra Pradesh police units and customer care centres of the West Bengal Electricity Distribution Company Limited. June 2017 saw the cyber-attack of **PETYA ransomware** where similar ransom, as in Wannacry, was asked in return for access of data which was locked by the hackers. Container handling functions at a terminal operated by the Danish firm AP Moller-Maersk at Mumbai's Jawaharlal Nehru Port Trust got affected. **Data theft at Zomato** in January, 2018, stole the data, including names, email IDs and hashed passwords of 17 million users was stolen by a hacker who demanded that the company must acknowledge its security vulnerabilities and put up the data for sale on the dark web. In July 2019– **Agent Smith malware** infected 15 million android devices in India. It was disguised as a Google-related app. In August 2019 RootAyyildiz **Turkish hacker** hacked the official website of the Bihar Education Department and "RootAyyildiz Turkish Hacker" claimed responsibility for posting messages praising Pakistan. In November 2020- Microsoft detected cyber-attacks from Russia and North Korea. Microsoft mentioned that these attacks were targeting the Covid-19 vaccine companies in India, France, Canada, South Korea and the United States. A Goldman Sachs backed firm Cyfirma also reported that Chinese hacker group APT 10 (also known as Stone Panda) had allegedly attacked the Covid-19 **vaccine manufacturers** in India. Cyfirma mentioned that there were links between the Chinese government and Stone Panda. In February 2021- Recorded Future (a U.S.-based cybersecurity firm) revealed an increase in suspected targeted intrusions against India from Chinese state-sponsored groups. At least **10 Indian power sector organisations** were targeted, in addition to two Indian ports. It mentioned that Mumbai power outages could be a cyber-attack as it was carried out by the Chinese state-sponsored group Red Echo. Chinese cyber-attacks in the past focussed on stealing critical information and not on projecting their cyber potential. But this cyber-attack on India was found to be different. Even in US, DarkSide ransomware attacked the Colonial Pipeline, the main supplier of oil to the U.S. East Coast, compelling the company to temporarily shut down operations. It was believed to be carried out by Russia/East Europe-based cybercriminals.

Blocking of Chinese Apps

The government's decision to block 59 Chinese apps in 2020, turned the spotlight on the vulnerability of internet with regards to national security. The PIB notification characterized these apps as 'malicious', citing several complaints against them for reportedly enabling unauthorized transmission of user data to servers situated 'outside India'. Till February 2020, 224 Chinese Apps have been banned through a series of government orders.

Recent Cyber-Attacks on Civilian Infrastructure Across the World:

1. **SolarWinds**: It was believed to be sponsored by Russia. It involved data breaches across several wings of the U.S. government, including defence, energy, and state.
2. **Hafnium**: It was an aggressive cyber-attack, by a Chinese group, and exploited serious flaws in Microsoft's software.
3. **Nobellium**: It was a phishing attack on 3,000 e-mail accounts, targeting USAID and several other organisations carried out by a Russia-backed group.

9.3. WHAT CAUSES AND FUELS CYBER-ATTACKS?

For cybercriminals and terror groups, the motive behind cyber-attacks is to **earn money** and generate an environment of **uncertainty, insecurity and fear**. The minimum setup cost makes cybercrime, the most preferred choice of attack. A cyber-attack gives a hacker access to critical economic data that can be sold for millions in the grey market. For example, IP thefts cost the US economy hundreds of billions of dollars annually and impact the R&D investment and innovation by US companies. Also, due to the inherent nature of cyber-attacks, they have become a **weapon of choice for countries engaged in modern warfare**. For instance, a Chinese attack on the weapon design system of the US allowed it to develop a competitive advanced defence system. It enabled the country to save millions of dollars and years of research and development by **spying** and **stealing sensitive/ confidential information** from US. Generally, one country attacks another country's data to serve its geopolitical interest in the region. Such attacks are aimed to cripple the governance structure of another country and influence it to act in a favourable way.

Data has become the world's **most precious commodity** and with the growth in the digital world, attacks on data and data systems are bound to intensify for various reasons. Generally, countries have **domestic laws** and agencies to punish cyber offenders. However, it is **difficult to punish**, if the attacker is located in another country as there are **no global rules** on cyberspace. Also, the advancement in technology has made the **traceability of hackers very difficult**. For instance, the hacking group, which carried out the ransomware attack on Colonial Pipeline (as discussed above), demanded ransom in bitcoins. Since transactions in cryptocurrency can't be traced so it has resulted in more such attacks. Moreover, **low entrance threshold** enables a curious person to learn and become a hacker. This allows him/ her to get into infrastructure, financial or military systems without leaving a trace. Rogue states and well-organised digital terrorist groups use such footloose hackers to invade diplomatic and strategic plans. For instance, the October 2020 cyber-attack shut down the electrical grid of Mumbai. The New York Times claimed this to be an attack carried out by China with the support of non-state actors.

9.4. WHY DO WE NEED CYBERSECURITY?

Over the years, **Information Technology** has transformed the global economy and connected people and markets in ways beyond imagination. With the IT gaining centre stage, nations across the world are experimenting with innovative ideas for economic development and inclusive growth. An increasing proportion of the world's population is migrating to cyberspace to communicate, enjoy, learn, and conduct commerce. It has also created new vulnerabilities and opportunities for disruption. As per the Kantar report, India's internet base has already breached the 500 million mark. It was likely to reach 627 million by the end of 2019. This has generated huge volumes of data. Also, rise of **digital platforms like UPI, GSTN, e-Office** has disproportionately increased the dependence on cyber infrastructure. There has also been an increased usage of e-learning- NPTEL, SWAYAM, Khan Academy, Udemy, Coursera and state specific e-learning classes like First Bell of Kerala, etc. COVID has also transformed traditional classrooms to online classrooms, thereby increasing the screen time of the students and making them more vulnerable to cyber-attacks. Hence, there is a need to protect the data and privacy of data of millions of users.

As per a report by the internet solutions provider Symantec, India is the **third most vulnerable country** in the world in terms of cybersecurity threats. According to CERT-IN, India experienced one cybercrime in every 10 minutes in the first half of 2019. Further, A National Crime Record Bureau report has also pointed out that cybercrimes reported in India rose by 19 times between 2005 to 2014 and by 77% from 2016 to 2017. India is **not just a victim** of cyber-attacks but is **also a perpetrator** and secures a spot amongst the top 10 spam sending countries in the world alongside the USA. The cyber security threats come from a wide variety of sources and cause disruptive activities that target individuals, businesses, national infrastructure and governments alike. Cyberspace has emerged as the **5th arena of war** (after land, air, water and space). Further, cyberspace has also allowed the **terrorist groups to stay anonymous** and propagate their nefarious activities (for example-propagating anti-state propaganda by radicalising the public). Thus, secured cyberspace is an integral part of strategic and **national security**.

Nations around the globe are concentrating on cyber defences to protect military and strategic targets, whereas the priority to protect civilian infrastructure is being overlooked. The use of '**Zero-day software**' that earlier existed only for the military domain now exists outside the military domain too. A **zero-day attack** (also referred to as Day Zero) is an attack that exploits a potentially serious software security weakness that the vendor or developer may be unaware of. It has the capability to **cripple a system and could lie undetected** for a long time. **The most infamous Zero-day software is Stuxnet.** It almost crippled Iran's uranium enrichment programme. Also, the **distinction between military and civilian targets is increasingly getting erased**. For instance, the **2012 cyber-attack on Aramco**, employing the Shamoon virus, had wiped out the memories of 30,000 computers of the Saudi Aramco Oil Corporation. Moreover, cyber-attacks on unconventional sectors have increased. For instance, banking and financial services were most prone to ransomware attacks, but oil, electricity grids, and lately, health care, have begun to figure prominently. Compromised 'health information' is proving to be a vital commodity for use by cybercriminals. The available data aggravates the risk not only to the individual but also to entire communities.

Instances of foreign governments interfering in the electoral process are also being reported. The **Cambridge Analytica** incident proves that **India is no exception to this trend**. This is a serious threat to national sovereignty and political stability. Telecom equipment and networks used for provisioning of telecom services are also prone to spyware/ malware etc., emanating from the equipment itself or embedded software contained in it. For example, a Report of Permanent Select Committee on Intelligence of US Government has pointed towards security threat from Chinese telecom equipment like Huawei. The concerns are over a perceived security risk posed by Huawei to countries it is operating in. As per a report in Bloomberg, Vodafone had identified hidden backdoors in the software that could have given Huawei unauthorised access to the carrier's fixed-line network in Italy. As a consequence, India kept the company out of 5G trial participants in May 2021, even though Huawei was willing to sign a "no back door" pact with the Indian government to assuage potential security concerns. Most equipment and technology for setting up cyber security infrastructure in India is currently procured from global sources. These systems are vulnerable to cyber threats just like any other connected system. While such disruptions are yet to cause damage worldwide, they serve as a wake-up call to the authorities concerned to initiate measures to improve the security and stability of cyberspace in terms of their own security. Also, Right to Privacy being a fundamental right (K.S Puttaswamy Case), puts the responsibility on the government to safeguard the privacy of an individual from various cyber-attacks.

Cambridge Analytica is a customer research and targeted marketing firm which was accused of harvesting data of people from Facebook and then using it to sway election results in US, supporting the candidacy of Donald Trump. An enquiry based on a complaint by the Indian Ministry of Electronics and Information Technology, further revealed that the company illegally collected data of approximately 5.62 lakh Facebook users from India as well.

Q. Cyberwarfare is considered by some defence analysts to be a larger threat than even Al Qaeda or terrorism. What do you understand by Cyberwarfare? Outline the cyber threats which India is vulnerable to and bring out the state of the country's preparedness to deal with the same.
(UPSC 2013)

9.5. CHALLENGES TO CYBER-SECURITY IN INDIA

Internet has become cheaper and more affordable and even reached the rural India where a large chunk of our population resides. This has resulted in **increased use/penetration of mobile technology and internet** with the internet usage in the country exceeding half a billion people. The **ICUBE 2018** report that tracks digital adoption and usage trends in India, noted that the number of internet users in India has registered an **annual growth of 18 percent** and is estimated at 566 million as of December 2018, a 40 percent overall internet penetration. Thus, **greater penetration** of internet reveals **greater vulnerability** in cybersecurity domain as large chunk of population is **not aware about cybersecurity practices**. The private sector is also culpable in its failure to report and respond to breaches in digital networks. Interpol data says that less than 10 % of such cases are registered with law enforcement agencies.

With varying income groups in India, not everyone can afford secure phones which are generally expensive. In US, mobile company Apple which manufactures iPhones having higher security norms, has over 44% market share. However, in India, iPhones are used by less than 1% of mobile users. Thus, Indians mostly use such devices where security infrastructure is weak and are easily susceptible to click on spam links because of being less digitally literate and aware. Lack of awareness regarding cyber security in the public makes them more susceptible to data misuse, frauds, hacking incidents on the internet where their data is used for purposes about which they have no prior information.

With the rapid pace of technology development, tools and forms of cyber-attacks are also evolving. This makes developing cyber-security products to cater to the present risks difficult. It is generally seen that attack technology outpaces defence technology, Botnets, DOS (Denial of Service) attacks have become so sophisticated that they penetrate through the existing security architecture, thus breaching the layers of protection. The **fourth industrial revolution** is leading to a fusion of technologies that is **blurring the lines between the physical, digital, and biological spheres**. Technologies like artificial intelligence, machine learning, internet-enabled devices and big data have complicated the cyber-attack ecosystem.

Traditionally, Indian cybersecurity is not something on which enough emphasis has been paid and this practice continues till date. Even in commercial offices, antivirus or such protection apps are considered to be unnecessary expenses. Moreover, lack of **cyber-security specialists** is another major concern. Nasscom has projected, India would need **1 million cyber security experts** by 2020. These cyber security specialists can avert any threats before they happen, or deal with them promptly and create such infrastructure and push systems forward which can avert future cyber-attacks. However, it is seen that governments also outsource cyber security to a select few private firms rather than having specialists and experts on its payroll. Also, lack of skills to deal with cyber-attacks in Indian IT professionals and lack of enough emphasis on data protection and backup creates greater challenges for India.

Cities are adopting new technologies and with the government's announcement of setting up 100 smart cities, cyber security will be an important component. Newer technologies along with faster and easier connectivity will allow such cities to use resources in an optimum manner, save money and provide better services to their citizens. Yet, whether smart or not, cities are bound to face numerous cyber security threats. These problems could have a direct impact on government, residents and the companies and organizations doing business there. The growing importance of cyberspace in critical applications, such as-

health, education, finance etc. has made the critical infrastructure vulnerable as well. Cyber security in cities is therefore, extremely important, but we are yet to fully realize the risk. Even governance is vulnerable to cyber threats. For example, initiatives like Aadhaar, MyGov, Government e-Market place, DigiLocker, BharatNet, Skill India are all prone to digital attacks.

There are **legal and policy issues as well.** National Cyber Security Policy has laid down a comprehensive framework regarding principles to be followed in the cyber security ecosystem. However, it does not include actionable or implementable steps. Moreover, a single IT Act is inadequate to deal with the different aspects of cyber security viz. cyber law, cyber security, cyber-crimes etc. The IT Amendment Act has also made several offences bailable and therefore reduced the conviction rate. The laws are such that even if the culprit is arrested, it's hard to prove the crime. The government's push for e-governance, the ever-expanding e-commerce sector and the booming social media platforms have generated large volumes of data of Indian citizens. But India still lacks a comprehensive data protection law.

9.6. ROLE OF MEDIA AND SOCIAL-NETWORKING SITES IN INTERNAL SECURITY

Social Media can be defined as any **web or mobile based platform** that enables an individual or agency to communicate interactively. It enables exchange of user generated content via blogs, discussion forums, Facebook, Twitter and other social networking sites. Social media has definitely made us closer to other parts of the world. Its reach, impact and potential in a globalized world is no longer contested. WhatsApp has become important for rural users, as it helps them connect at low cost to family members far away and send pictures of their products to clients across India. The power of social media is that it can enforce necessary change. These platforms have provided an interface to the public, to raise their voice against injustice and inequality, for aggrieved sections like the fight **for LGBTQ rights**, for providing help and disseminating information during disasters and also for grievance redressal. They have also been increasingly adopted by politicians, political activists and social movements as a means to **engage, organize and communicate** with citizens. Since these platforms are majorly used by the young population, it has empowered them by making information accessible and helping in creating informed public opinions. Many people also run educational, motivational channels on YouTube, thereby educating and inspiring a huge bunch of people. But what happens when the information used to form such public opinion is actually misinformation- a piece of unverified news, carefully crafted to be presented as alternate facts and drive the propaganda machines. It undoes all the positive work that social media has done until now. Social media is thus a fascinating phenomenon which presents both **challenges** and opportunities to governments and law enforcement agencies across the spectrum.

Social media companies exploit the social environment as well and the fundamental business model of such companies like Facebook poses some serious concerns. Their goal is to **collect** as much **personal information** on individuals as possible and then use this information to sell highly **targeted advertising** to companies. Data of millions is taken and used where people knowingly or unknowingly give consent. Individuals often share their data without being aware of it or understanding the implications of privacy terms and conditions. Data of public is often misused and false opinion building practices are undertaken. This is particularly nefarious, because these companies influence how people think and behave, without them even being aware of it. Such level of data collection and manipulation represents the concentration of enormous power in the hands of a single corporation. The Cambridge Analytica scandal has highlighted how this power can be used by a small group of people with an agenda to foster polarisation, radicalisation and undermine the integrity of democratic elections.

We live in a world where we aren't only the consumers of information but creators as well. Free service has given access to everyone to post whatever they want and thus create a trend in fake

news spreading like wildfire. Everyone is in a **hurry to Like/Share/Comment** rather than checking the authenticity of the news. When doctored news comes from official or verified channels, then it invokes strong emotional responses as well. Moreover, the number of users using social media platforms and internet are ever increasing and the volume of traffic is huge. This makes it difficult to find out the origin of the information. Moreover, trolling of women has brought to the fore the disturbing reality of online violence and abuse women face in India. There are also issues of cyber bullying and online harassment. Researchers have found that **hyper-networking** also leads to negative health behaviour like **laziness, obesity, depression, drug abuse, isolation** or in the worst cases it may even lead to **suicide**. For example, **the 'Blue whale challenge'** saw detrimental consequences on the mental and psychological health of many young individuals. Social networking sites also pose major challenges in **financial and organized crime** which destabilizes the system. It creates a threat to a company's security because of what employees might disclose and they are on prime target for cyber criminals. Such sites enable fraudsters to take excellent opportunity to become wealthy by selling deceiving schemes.

Spread of fundamentalism and terrorist ideology via social media and internet is another major concern. Increased use of cyberspace by terrorists to defraud gullible population, brainwash and indoctrinate them with their **vendetta, spreading propaganda and misinformation, incitement and recruitment** of extremist elements, coordination of plans of attack, communication with cells through the internet has become very simple in the past few years. These groups now have their own websites where they can convey their propaganda and where they advise their readers and followers not to trust the media which are seen as the enemy. This is a major concern for agencies dealing with cybersecurity around the world. WhatsApp, Facebook, Twitter and similar social media sites have been seen to be a very effective medium in spreading terrorist ideologies. For example, 6 youths were caught by NIA in 2016, who used social media to connect to ISIS and be a part of their organization. Internet is increasingly being used to target the youth through online radicalization for conducting lone wolf attacks and for recruitment, thus making the spread of terrorist activities more diffused, widespread and anonymous. For example, Mehdi Masroor Biswas arrested from Bangalore after a tip from UK, operated the most influential twitter handle of ISIS (@shamiwitness), for over a year. Militants in Kashmir are using social media to attract the people to their ideology and also to fuel unrest and violence. The case of "Facebook militant" Burhan Wani is an important example. Moreover, digital messaging using social media can contribute to social unrest and clashes. For example, 2012 mass exodus of people belonging to north east and 2013 Muzaffarnagar riots based on viral videos and spread of misinformation on social media. Even television propaganda programmes like **UPSC jihad** are an attempt to malign the social fabric of the nation and create unnecessary controversies based on unfounded data.

The other national and international users such as the political parties, NGO's, hackers also pose a serious threat using the internet. For example, during the **civil turmoil in the Arab Spring uprising**, various governments were threatened through social media. China is also known to monitor the online activities of at least 1,350 Indians, including key politicians and some high-profile individuals in the country. The list includes former presidents, prime ministers, key businessmen, and even Bollywood actors. Not just external influences, but media also needs to tread cautiously while covering sensitive events and **emergency situations like the Kargil war and 26/11 attacks,** wherein domestic media coverage played into the hands of the enemy, who used the real time news for their advantage. It is therefore of utmost importance that the government steps in to regulate both news media and social media and nudge these companies to develop their **own internal mechanisms** to counter such events. The first step was taken by the Ministry of Information and Broadcasting in 2018-19, when it released a notification criminalizing fake news circulation. However, it was soon withdrawn due to a conflict between freedom of speech and expression and the government's role in handling fake news.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Social Media intermediaries, with registered users in India above a notified threshold, have been classified as Significant Social Media Intermediaries (SSMIs). SSMIs are required to appoint designated personnel for compliance of these rules. SSMIs need to enable the identification of the first originator of the information on its platform under certain conditions. SSMIs need to deploy technology-based measures on a best-effort basis to identify certain types of content. All intermediaries are required to provide a grievance redressal mechanism for resolving complaints from users or victims. A three-tier grievance redressal mechanism has been prescribed.

* Discussed in more details under section 9.6.1

Social media platforms are benefitting from user traffic. They must be bestowed with responsibility for threat emanating from their platforms. They claim that they are merely distributing information. But the fact that they are near monopoly distributors makes them public utilities and therefore they should be subjected to more stringent regulations, aimed at preserving competition, innovation, and fair and open access. Recent laws directed at social media have that changing in Germany, wherein social networks could pay up to $60 million in fines if hate speech isn't removed within 24 hours. Similar laws can be framed in India also. Social networks also need to enhance their own governance, continue to refine the algorithms, use more "friction" like warnings and notifications for suspicious content, expand human oversight, adjust advertising, and continue to share knowledge with other networks to reach those goals. For instance, Facebook introduced guidelines on how to identify fake news, WhatsApp incorporated a new feature wherein any message could not be forwarded to more than 5 chats at one go. India also needs to have a legal framework for data protection. It will create a vital and necessary framework against which rights and responsibilities can be articulated, and digressions thereof evaluated. Experts have pointed to the importance following basic cyber hygiene and a periodic review of the security facets of one's profile on various web platforms, especially on social media, where users tend to share personal information. Awareness programs can be held in schools, colleges, universities to educate the people about its judicious use.

There should be judicious use of social media. But we will have to mull steps to check its misuse for creating internal security threat to the nation. Social media ought to be used in the correct manner for creative or productive purposes so that it is progressive to mankind and society at large, rather than regressive. **Social media analysis generated intelligence or SOCMINT** is being developed as a successful model in many countries abroad to isolate hotspots or subjects that go viral and is used as a predictive tool. Many fact checking agencies and websites like AltNews already perform the tireless work of checking the authenticity of all major trending news items on online platforms. Policing systems also need to update so that they can cater to the new age realities. Police need to be tech savvy so that they are aware of the threats emanating from the social media platforms. For example, the Mumbai Police has launched a project called "Social Media Lab", the first of its kind in the country. Further reform steps to ensure cyber security have been discussed in the last section.

How to Spot Fake News?

First, we need to **Check the source, i.e.** check the web address for the page you are looking at. Sometimes, fake news sites may have spelling errors in the URL or use other domains extensions like- 'infonet' etc.

Next check the author, research about the author to see if they are credible- for instance, are they real, do they have a good reputation, or do they have an area of expertise on that topic, or do they have any hidden agenda, or can they have a biased motivation.

Then **check other sources,** see if there are any other reputable news or media outlets reporting on the same story? Always **maintain a critical mindset,** as a lot of fake news is cleverly written to provoke strong emotional reactions such as fear or anger. Ask yourself if the story is promoting a particular cause or agenda or trying to force you to click another website. Also, **check the facts,** reports with false information often quote incorrect dates or altered timelines, so it is a good idea to check when the article was published. Always **watch for your own biases,** as we all have biases which could influence the way we respond to certain news articles. Social media can create **echo chambers** by suggesting stories that match our existing browsing habits, interests and opinions. The more we read from diverse sources and perspectives, the more likely it is that we can draw accurate conclusions. Finally **use a fact-checking site**: If we are not sure whether an article is authentic or not, pause and rethink before sharing it with others. We can also use fact-checking websites to find the authenticity of the news item.

Campaigns by social media platforms:

WhatsApp launched a nationwide campaign called "Share Joy, Not Rumours" to help prevent the spread of rumours and fake news. Facebook launched #SocialForGoodCampaign to address issues such as cyber bullying, mental wellbeing, and entrepreneurship and was targeted primarily at young users. Twitter launched #PowerOf18 campaign to encourage youth to contribute to public debate and participate in civic engagement in the election season.

9.6.1. New IT Rules 2021 for Social Media

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 came into force in India in May 2021. (After releasing the IT Rules in February, 2021, the government had provided 3 months' time for social media platforms to adhere to the rules.) The new IT rules have been framed to address Social Media, Digital Media, and OTT platforms in a specific manner.

Provisions

Social media companies are prohibited from hosting or publishing any unlawful information. This information is "in relation to the interest of the sovereignty and integrity of India, public order, friendly relations with foreign countries, etc.". If such information is hosted or published, the government can take down such information within 24 hours. The user will be given a notice before his/her content is taken down. The provision of **traceability** mechanism requires the social media platforms to compulsorily identify the first originator of the information in India, upon government or court order. Social media platforms are now classified into two categories. 'Social media intermediaries' – Platforms that have a limited user base; and 'Significant social media intermediaries' – These are the platforms with a large user base. The significant social media intermediaries have to follow few additional measures like having a physical contact address in India, appointing a Chief Compliance Officer, Nodal Contact Person, and a Resident Grievance Officer in India - all of whom should be Indian residents. The Nodal Contact Person would be responsible for 24×7 coordination with law enforcement agencies. The Resident Grievance Officer would have to acknowledge the complaint within 24 hours, and resolve it within 15 days of receipt.

However, there are certain **issues** surrounding the New IT Rules 2021 for Social Media platforms. The rules require tracing the information back to the source which is against some social media policies. For example, WhatsApp claims that the traceability clause is in conflict with their policy of end-to-end encryption. If they accept, then their services cannot remain end-to-end encrypted. The rules are also against the **Doctrine of Proportionality**. It is a doctrine which examines whether administrative processes violate the principle of the action not being more drastic than it ought to be for obtaining the desired result. Under this doctrine, question arises if the executive should achieve the goal (i.e. elimination of the threat to security and sovereignty of the nation by social media) by adopting drastic measures such as tracing the messages. Moreover, implementation of New IT Rules might allegedly increase political control of social media companies and posts on social media. This is because the New IT Rules for social media do not have legal backing.

Since new IT rules are framed by bureaucrats, there might be wider use of discretionary censorship. Also, non-compliance with new rules would take away the protection granted to social media intermediaries under Section 79 of the IT Act. This section mentions that any intermediary shall not be held legally or otherwise liable for any third-party information, data, or communication link made available or hosted on its platform.

Due to the above limitations, WhatsApp filed a case in Delhi High Court, against the enforcement of New IT rules. The new rules are also seen to be curtailing free speech on digital platforms. The Supreme court in its Puttuswamy case (Right to Privacy) judgment mentioned that any law that impacts the fundamental right is void. Further, this iteration was also mentioned in the Anuradha Bhasin case on Internet freedom. Critics argue that implementing the new IT Rules for social media will violate the said judgment and its provisions. The **social media companies** are also of the view that the rules were notified in a short time without much public and stakeholder consultation. Companies like Facebook have expressed their intention to comply with the rules, however they have requested to engage with the Government on certain genuine concerns before ensuring compliance.

The **Central government** has opined that social media companies are currently not classified as legally intermediaries. Under section 2W of the IT Act, the definition of **intermediary does not include social media companies**, while it mentions internet service providers, online auction sites, online marketplaces, etc. as intermediaries. The government has mentioned that the social media companies would be treated as an intermediary if they adhere to the new IT rules. Also, these platforms use curated content for money-making and do not undertake editorial regulations. The new IT rules have thus been aimed to change that perception. From May 2021 onwards, the content on social media platforms would also follow Indian publishing rules and regulations, just like the print media. The government has underlined that the new IT rules on social media would benefit the society at large. Once the rules come into effect, users' **personal photographs, personal data would remain safe** with the user and ensure **Right to Privacy**. Children and women would also feel safe and secure on social media. The chances of **cyber-bullying, exposure to obscene content, and harassment** would reduce on social media platforms. If the rules adhered to strictly, then any posts promoting a particular race, sex, caste, religion would reduce in time. This would promote India as a multi-cultural society. The social media companies would also have to remove any posts that promote radicalism, online terrorism, violence over social media. Thus, it would weaken India's internal and external threats.

The New IT rules for social media alter the entire social media platform's function, responsibility, compliance, and user rights. But to get the desired outcome the rules alone are not sufficient. It requires legislative backing to regulate social media companies in India. The government can enact a draft bill on the **regulation of digital platforms** after the due consideration of the upcoming judgment of the Delhi High Court in the WhatsApp case. This will become a watershed moment that will transform the digital ecosystem in India. The government can also enact a data protection law in line with the **GDPR** (General Data Protection Regulation of European Union). This would address majority of the issues with the social media platform. Further, it would force social media platforms to store data within India itself.

Q1. What are social networking sites and what security implications do these sites present? **(UPSC 2013)**

Q2. Religious indoctrination via digital media has resulted in Indian youth joining ISIS. What is ISIS and its mission? How can ISIS be dangerous for the internal security of our country? **(UPSC 2015)**

Q3. Use of the internet and social media by non-state actors for subversive activities is a major security concern. How have these been misused in the recent past? Suggest effective guidelines to curb the above thre at. **(UPSC 2016)**

9.7. PROGRAMMES AND INITIATIVES

Cyberspace is becoming a new battlefield. Successful attacks have caused significant financial

loss and other problems. Cyber security is thus very crucial for digital governance and its broad ecosystem. Government has therefore taken several steps to prevent and mitigate cyber security incidents.

9.7.1. Policy Measures

A. National Cyber Security Policy, 2013

It is a policy framework to create a secure cyberspace ecosystem and strengthen the regulatory framework. It was formulated in the aftermath of the revelation made by **Edward Snowden** about US NSA spying on Indian users. This made India one of the first few countries to have a dedicated **cyber security policy** with the recognition of the fact that cyber security is an **integral part of national security.** The National Cyber Security Policy has been prepared in consultation with all relevant stakeholders, user entities and public. The policy aims at facilitating creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders' actions for protection of cyber space. It aims to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation. The objectives of the policy include **Creation of secure cyber ecosystem** in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy. Also, compliance to **global security standards** to create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people). Further, strengthening the **regulatory framework** for ensuring a Secure Cyberspace ecosystem. In addition, Creation of National Critical Information Infrastructure Protection Centre (**NCIIPC**) to enhance the protection and resilience of Nation's critical information infrastructure by operating a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources. Steps to ensure **indigenization of technologies** in order to develop suitable indigenous security technologies through frontier technology research, solution-oriented research, proof of concept, etc.

Robust **infrastructure for testing and validation** to improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products. Ensuring **human capacity development** to create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training. Measures to **safeguarding privacy** to enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cybercrime or data theft. Finally, **tackle cybercrime** to ensure effective prevention, investigation and prosecution of cybercrime and enhancement of law enforcement capabilities through appropriate legislative intervention.

The policy, however, did not specify what all came under the critical information infrastructure. It also lacked detailed implementation guidelines and plan of action. The provisions which were mandatory in the policy needed deeper analysis based on the experience of other countries and the Indian context. For example, US had to withdraw its cyber security bill which mandated security standards as the industry found them difficult and costly to implement. In this process, they lost crucial time in making their critical information infrastructure more secure, thereby making them vulnerable to subsequent cyber-attacks. Experts were also of the view that too much of government intervention through regulations could undermine business innovation, making it uncompetitive. The better approach could have been to incentivize the private sector to invest in security beyond what is required by business requirements, through government funding, tax reliefs, awards & recognition, liability protection, cyber insurance, etc. Also it was appreciable that one of the objectives of the policy was to safeguard the privacy of citizen's. However, no specific strategy or activity

to achieve this objective had been mentioned in the policy. The policy did not even seem to fully establish the leadership role that India should play in the International arena, as a hub of vast online data.

What are Critical Information Infrastructures?

Critical Information Infrastructure (CII) is defined as those facilities, systems or functions whose incapacity or **destruction** would cause a **debilitating impact on national security**, governance, economy and social well-being of a nation. Examples: Reserve Bank of India (RBI), Nuclear Power Plants, Indian Space Research organization (ISRO), Department of Atomic Energy, transport, electricity, etc. **National Critical Information Infrastructure Protection Centre** (NCIIPC) is an organisation of the Government of India created under Sec 70A of the Information Technology Act, 2000 (amended 2008). It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection.

Q. Considering the threats cyberspace poses for the country, India needs a "Digital Armed Force" to prevent crimes. Critically evaluate the National Cyber Security Policy, 2013 outlining the challenges perceived in its effective implementation. **(UPSC 2015)**

B. Draft National Encryption Policy 2015

The draft policy aimed at enabling information security environment and **securing transactions in cyberspace** for individuals, businesses, government including nationally critical information systems and networks. The mission was to provide confidentiality of information in cyber space, protection of sensitive or proprietary information and ensuring continuing reliability and integrity of nationally critical information systems and networks. It planned to synchronize with the emerging global digital economy / network society and use of encryption for ensuring the security / confidentiality of data without unduly affecting public safety and national security. It also encouraged wider usage **of digital signature by all entities** including government for trusted communication, transactions and authentication.

According to the draft policy, all citizens were required to **store the plain text of the encrypted messages for 90 days** and provide it to law enforcement agencies as and when required. All vendors of encryption products would need to **register their products with the designated agency** of the government and all encryption technology used in India would be cleared by the government. Government would maintain a list of all encryption technologies and only those technologies which were on the list could be used in the country. It implied that government would know every encryption technology used in India. Common use Web-based applications and social media sites such as WhatsApp, Facebook and Twitter were exempted. The encryption products being used in internet-banking and payment gateways under direction of the RBI and those being used for e-commerce and password-based transactions, were also exempted. **Research and development programs** would be initiated for the development of indigenous algorithms and manufacture of indigenous products for encryption, hashing and other cryptographic functions.

However, the **biggest concern** of this draft policy was that users and organizations would "on demand" need to store all communication in plain text for 90 days from the date of transaction and make it available to law enforcement agencies. Most of the users in India do not know the meaning of plain text and in such a case they could be held liable for not storing their encrypted data in plain text format. Thus, almost everyone using the internet would find themselves in violation of these rules. Also, service providers located within and outside India, using encryption technology for providing any type of services in India, would need to enter into an agreement with the government. This was **seen as impractical** as there are many service providers around the world that use encryption. It would be highly **unrealistic** for all of these to enter into an agreement with the Indian government. Moreover, keeping a copy of the data would require huge storage and that would come at a cost. There was also an apprehension that the policy would start a new **"registration raj"**, now that all encryption technologies that could be used in India would need to be certified and listed by the concerned

agencies. For companies that stored private data it would mean storing passwords in plain text, which meant that private and confidential data would remain unencrypted and hence vulnerable for 90 days. Given the concerns raised by the policy, it was withdrawn soon after.

C. Crisis Management Plan

It has been formulated as per guidelines of Ministry of Electronics and Information Technology, for countering cyber-attacks and cyber terrorism which will be implemented by all Ministries and Departments of the Centre and the state governments in critical sectors so as to deal with sudden crisis situations which can disrupt the functioning of the organisation.

D. Cyber Surakshit Bharat Initiative

Launched in 2018, it aims 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. Guidelines for CISOs regarding their key roles and responsibilities for securing applications / infrastructure and compliance have been issued. It also involves conducting **regular training programmes** for network / system administrators and CISOs of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber-attacks. 1.14 Lakh persons have to be trained through 52 institutions under the Information Security Education and Awareness Project (ISEA) (to raise awareness and to provide research, education and training in the field of Information Security).

A **Chief Information Security Officer** (CISO) is the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

E. Cybercrime Volunteer Programme

The Ministry of Home Affairs launched the **Cybercrime Volunteer programme in 2020**. The programme aims to bring together citizens to contribute to the **fight against cybercrime** in the country. The scheme also aims to assist State/UT in their endeavour to curb cybercrimes. Under the programme, citizens can register themselves as **cyber-crime volunteers**. They will help the law enforcement agencies in identifying, reporting and removing illegal/unlawful online content. The program is a constituent of the National Cybercrime Ecosystem Management Unit. This unit is in turn a part of the Indian Cyber Crime Coordination Centre(**I4C**) scheme.

F. Other Measures

As per the guidelines of MEITY and MHA, **audit** of the government websites and applications prior to their hosting, and thereafter at regular intervals, has been made mandatory. Looking forward to becoming a secure cyber ecosystem, India has joined hands with several developed countries like the United States, Singapore, Japan, etc. These agreements will help India to challenge even more sophisticated cyber threats. In January 2018, the government announced its plans to introduce **Cyber Warrior Police Force (CWPF)**. It is to be raised on lines of Central Armed Police Force (CAPF) and responsible for conducting cyber security mock drills and exercises regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors.

In 2019, the government also announced a **National Mission on Interdisciplinary Cyber-Physical Systems** (NM-ICPS). The mission has allotted a budget of Rs 3,660 crore for five years, to strengthen the Cyber-Physical Systems(CPS). The Bureau of Indian Standards (BIS) has also launched the **Industrial Cybersecurity Standards** (IEC62443). This standard aims to address and mitigate current and future cybersecurity challenges, especially in industrial automation and control systems. But the government is yet to adopt the standards. Government has also launched the **online cybercrime reporting portal**, www.cybercrime.gov.in to enable complainants to report complaints pertaining to Child Pornography/Child Sexual Abuse Material, rape/gang rape imageries or sexually explicit content.

During the **12th India Security Summit on "Towards New National Cyber Security Strategy"**, many issues were discussed such as the protection of critical national infrastructure, emerging cyber threats- incidents, challenges and responses. Also, when Indian Prime Minister visited France

Cyber Dome Project

Cyber dome is a **technological research and development centre** of **Kerala** Police Department, conceived as a **centre of excellence in cybersecurity** for effective policing. It involves setting up of a high tech public-private partnership centre of collaboration for different stakeholders and handling of cyber-crimes in a proactive manner. The IT industry would be contributing in terms of expertise, manpower, hardware, software, training, etc. on a pro-bono basis. Also, most of the crew of ethical hackers (or white hats), expert coders, youth prodigies skilled in software, law enforcers and civilian volunteers would be offering their services for free. These would act as State law enforcement's first line of defence against a range of online threats. The primary objective of Cyber dome is to **prevent cybercrimes** through developing a cyber-threat resilient ecosystem in the state. It makes collective coordination among the Government departments and agencies, academia, research groups, non-profitable organizations, individual experts from the community, ethical hackers, private organizations, and other law enforcement agencies in the country with the aim of providing a safe and secure cyber world for each and every citizen.

Further, Cyberdome envisages to take **proactive measures against** the evolving **cyber threats**. In this regard Cyberdome regularly conducts **VPAT** (Voluntary Product Accessibility Template) in the government as well as the private domains and reports the same with mitigation strategy. In addition, CyberDome conducts **secure coding workshops** to equip the developers and IT admins of organisations to develop hackproof and secure websites. Also, strong collaboration of Cyberdome with the RBI, banks, payment gateways etc., can help **minimise the financial frauds**. Moreover, Cyberdome has also started a ransomware school to understand, analyse and mitigate ransomware infections, create SOPs to deal with ransomware, and create awareness in public as well as government departments about ransomware and associated precautionary steps. Thus, we can see that Cyberdome project will not only aid in checking financial frauds, threat to law and order etc., but will also prevent social crimes like eve teasing, online bullying, child pornography etc.

Q. What is the Cyber Dome Project? Explain how it can be useful in controlling internet crimes in India. **(UPSC 2019)**

in August 2019, India - France adopted a **cyber-security and digital technology** roadmap which aimed at expanding Indo - French bilateral cooperation in cyber security sector. Moreover, India currently is one of the fastest growing market of electronics in the world, and therefore, the **National Policy on Electronics** aims to address the issue with the clear-cut goal of transforming India into a premier Electronic System Design and Manufacturing (**ESDM**) hub. Promotion of domestic manufacturing and exports in the entire value-chain of ESDM will help reduce security risks from foreign made chip-sets and other electronic devices and components.

A **National Cyber Security Strategy 2020** is being formulated by the Office of National Cyber Security Coordinator at the National Security Council Secretariat, 2020, based on the 3 pillars- **secure, strengthen and synergise**. It aims to improve cyber awareness and cybersecurity through more stringent audits. Empanelled cyber auditors will look more carefully at the security features of organisations than are legally necessary now. There will be table-top cyber crisis management exercises regularly to reinforce the idea that cyber-attacks can take place regularly. It also calls for an index of cyber preparedness, and monitoring of performance. A separate budget for cybersecurity is suggested, as also to synergise the role and functions of various agencies with the requisite domain knowledge.

9.7.2. Legislative Measures

'Police' and 'Public Order' are State subjects as per the Constitution of India. States/UTs are primarily responsible for prevention, detection, investigation and prosecution of crimes through their law enforcement machinery. The Law Enforcement Agencies take legal action as per provisions of law against cybercrime offenders. Some of the central laws are:

A. Information Technology Act, 2000

The Act regulates use of **computers, computer systems, computer networks** and also data and information in electronic format. The bill was introduced in May 2000 and received assent of President in August 2000 and became an Act. This Act aims to provide for a legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. It also aims to provide **legal infrastructure for e-commerce in India**. The Act covers a broad range of offences including **child pornography, cyber terrorism** etc. Section 75 of the Act empowers the government to punish people located outside India who are accused of any offence. Chapter II deals with use of **digital signature** to authenticate an electronic record. Chapter-III of the Act details about **electronic governance** and provides inter alia amongst others that where any law provides that information or any other matter shall be made available in an electronic form; and accessible so as to be usable for a subsequent reference. Chapter-IV of the said Act gives a scheme for **regulation of certifying authorities**. The Act highlights the need for recognizing foreign certifying authorities and it further details the various provisions for the issue of license to issue digital signature certificates.

Chapter-IX of the said Act talks about **penalties and adjudication** for various offences. The penalties compensation not exceeding Rs.1,00,00,000 to affected persons. The Act talks of appointment of any officers not below the rank of a Director to the government of India or an equivalent officer of state government as an adjudicating officer who shall adjudicate whether any person has made a contravention of any of the provisions of the said Act or rules framed there under. The said adjudicating officer has been given the powers of a civil court. Chapter-X of the Act talks of the **establishment of the Cyber Regulations Appellate Tribunal,** which shall be an appellate body where appeals against the orders passed by the adjudicating officers, shall be preferred.

Chapter-XI of the Act talks about **various offences** and the said offences shall be investigated only by a police officer not below the rank of the Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, which is obscene in electronic form, and hacking.

The Act also provides for the constitution of the **Cyber Regulations Advisory Committee**, which shall advice the government as regards any rules, or for any other purpose connected with the said act. The said Act also proposes to amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934 to make them in tune with the provision of IT Act.

B. The Information Technology (Amendment) Act 2008

The Information Technology (Amendment) Act, 2008 amended the IT Act 2000 and received the assent of the President on 5th February 2009. It deals with **data protection**, with no specific reference to data protection in 2000 Act, the ITA 2008 introduced two sections addressing data protection, Section 43A (Compensation for failure to protect data), and Section 72A (Punishment for disclosure of information in breach of lawful contract. Section 67C refers to the **preservation and retention of information by intermediaries.** According to Central government, any intermediary who intentionally or knowingly contravenes the provisions shall be punished with an imprisonment for a term which may extend to 3 years and shall be liable to fine. Section 69 gives power to issue directions **for interception or monitoring or decryption of any information** through any computer source. Section 69B authorizes to **monitor and collect traffic data or information** through any computer resource for cyber security.

The IT (Amendment) Act,2008 from an overall perspective introduced **remarkable provisions and amendments** to facilitate the effective enforcement of cyber-law in India. Section 46(5) of the IT Act is a welcome provision that empowers the Adjudicating officers by conferring powers of execution at par with a civil court. New cybercrimes have been incorporated under chapter XI as offences under the amended Act, to **combat growing kinds of cybercrimes** particularly, serious crimes such as child pornography, and cyber terrorism. The intermediaries have been placed under an obligation to maintain and provide access to sensitive information to appropriate agencies to assist in solving cybercrime cases under Section 67C, Section 69. However, there are some challenges that cyber law enforcement teams would

be faced with. The power of interception of traffic data and communications over internet would need to be exercised in **strict compliance of rules** framed under the Act. Power for blocking websites should also be exercised carefully and should not transgress into areas that amount to unreasonable censorship. Many of the offences added to the Act are **cognizable but bailable** which increases the **likelihood of tampering of evidence** by cybercriminals once released on bail. The police must therefore play a vigilant role to collect and preserve evidence in a timely manner. In order to achieve this, police force should be well equipped with forensic knowledge and trained in laws to effectively investigate cybercrime cases.

9.7.3. Bodies and Organizations to Deal with Cyber-Attacks in India

A. CERT-In (Cyber Emergency Response Team -India)

Established in 2004, CERT-In functions under MeitY and is mandated to serve as the **national agency in charge of cyber security**, under the IT Amendment Act, 2008. CERT-In is India's response to cyber threats and all organizations providing digital services have been mandated to report cyber security incidents to CERT-In expeditiously. The purpose of the CERT-In is, to become the nation's **most trusted referral agency** for responding to computer security incidents as and when they occur. Its mission is to enhance the security of India's communications and information infrastructure through proactive action and effective collaboration. Since November 2012, DG of CERT-In is called the **National Cyber Security Coordinator** (NCSC). The 2017 budget made an announcement regarding CERT- FIN as well, for supervision and protection of the financial sector. However, as of 2021, it has not been established.

B. NTRO (National Technical Research Organisation)

NTRO is a technical intelligence agency under the **National Security Adviser** in the Prime Minister's Office, which was set up in 2004. It also includes National Institute of Cryptology Research and Development (NICRD). The agency develops technology capabilities in aviation and remote sensing, data gathering and processing, cyber security, cryptology systems, strategic hardware and software development and strategic monitoring. National Technical Research Organisation (NTRO), originally known as the National Technical Facilities Organisation (NTFO), is a highly specialised technical intelligence gathering agency. While the agency does not affect the working of technical wings of various intelligence agencies, including those of the Indian Armed Forces, it acts as a super-feeder agency for providing technical intelligence to other agencies on internal and external security.

C National Critical Information Infrastructure Protection Centre (NCIIPC)

NCIIPC is designated as the **National Nodal Agency in respect of Critical Information Infrastructure** (CII) protection. Any delay, distortion or disruption in the functioning of these CIIs can easily be led to political, economic, social or national instability. **Objectives of NCIIPC** includes delivering advice **to reduce vulnerabilities**. Also, Identifying all CII elements for notification. Further, **provide strategic leadership** and coherent government response. Also, to coordinate, share, monitor, collect, analyse and forecast threats.

Develop plans, adopt standards, share best practices and refine procurement processes. In addition, evolve protection strategies, policies, vulnerability assessment and auditing methodologies and plans for CII. Its job is also to **undertake R&D** to create, collaborate and develop technologies for growth of CII protection. Further its mandate also for CII protection and developing cooperation strategies. Issue guidelines, advisories etc. in coordination with CERT-In and other organisations. It is also expected to **exchange knowledge and experiences** with CERT-In and other organisations. NCIIPC has power call for **information and give directions** to CII.

D. Cyber Swachhta Kendra

Under the Digital India initiative, **Cyber Swachhta Kendra** was launched in 2017 for internet users to clean their computers and devices by wiping out viruses and malware. Cyber Swachhta Kendra or **Botnet Cleaning** and **Malware Analysis Centre** has been launched for providing detection of malicious programmes and free tools to remove such programmes.

E. National Cyber Coordination Centre (NCCC)

In 2017, NCCC was established with a mandate to **scan internet traffic and communication** metadata (which are little snippets of information hidden inside each communication) coming into the country to **detect real-time cyber threats**. It collects, integrates and scans [internet] traffic data from different gateway routers of major ISPs at a centralized location for analysis. The NCCC will generate **actionable reports/alerts** for proactive actions by the concerned (law enforcement) agencies.

F. Indian Cyber Crime Coordination Centre (I4C) – a 7-Pronged Scheme to Fight Cyber Crime

MHA has rolled out a scheme 'Indian Cyber Crime Coordination Centre (I_4C)' for the period **2018-2020**, to combat cybercrime in the country, in a coordinated and effective manner. Central Government has taken steps to spread awareness on cybercrime, issue cyber related alerts/ advisories, capacity building/ training of law enforcement officers/ judges/ prosecutors, improving cyber forensics facilities etc. to prevent cybercrime and expedite investigations. Indian Cyber Crime Coordination Centre (I4C) and the Cyber Police Force will be set up under the newly created **Cyber & Information Security (CIS) Division** of the Union Ministry of Home Affairs. CIS Division will have four Wings, namely Security Clearance, Cyber Crime Prevention, Cyber Security and Information Security Wings each headed by an Under-Secretary level Officer. An online portal for preparing, follow up and issue of advisory on financial fraud related matters is also in the offing. The scheme has the seven components with different mandates. **National Cybercrime Threat Analytics Unit** shall provide a platform for law enforcement personnel, persons from the private sector, academia and research organizations to work collaboratively in order to analyse all pieces of puzzles of cybercrimes. Threat Analytics Unit shall also produce cybercrime threat intelligence reports and organize periodic interaction on specific cybercrime centric discussions. Create multi-stakeholder environment for bringing together law enforcement specialists and industry experts. **National Cybercrime Reporting Portal** will work in tandem with already established investigation units at state and central levels as well as experts from different spheres to create expert investigation teams and will have the capability to respond in real time to rapidly changing cybercrime threat. Also, will be able to collaborate with partners to investigate cyber and cyber-enabled crime. **Platform for Joint Cybercrime Investigation Team,** with an objective to drive intelligence-led, coordinated action against key cybercrime threats and targets. This will facilitate the joint identification, prioritization, preparation and initiation of multi-jurisdictional against cybercrimes. **National Cybercrime Forensic Laboratory Ecosystem,** will ensure Forensic analysis and investigation of cybercrime as a result of new digital technology and techniques. Develop a centre to support investigation process. NCFL and associated Central Forensic Science Laboratory to be well-equipped and well-staffed in order to engage in analysis and investigation activities to keep-up with new technical developments, using which a completely new kind of cybercrime might have been committed. **National Cybercrime Training Centre** will be setup to focus on standardization of course curriculum focused on cybercrimes, impact containment and investigations, imparting practical cybercrime detection, containment and reporting trainings on simulated cyber environments. Development of Massive Open Online Course to be delivered on a cloud-based training platform. It will also focus on establishing Cyber Range for advanced simulation and training on cyber-attack and investigation of such cybercrimes. **Cybercrime Ecosystem Management Unit** to develop ecosystems that bring together academia, industry and government to operate, investigate a cybercrime basis established standard operating procedures, contain the impact of cybercrimes and respond to cybercrimes. Provide incubation support for development of all components of cybercrime combatting ecosystem. **National Cyber Research and Innovation Centre** to track emerging technological developments, proactively predict potential vulnerabilities, which can be exploited by cybercriminals. To leverage the strength and expertise of all stakeholders, be it in academia, the private sector or inter-governmental organizations. Create strategic partnerships with all such entities in the area of research and innovation focused on cybercrimes, cybercrime impact containment and investigations.

Online Surveillance as a Disguise for National Security?

Digital rights and freedom are indicators of democracy. Internet enables individuals to **seek, receive and impart information** and ideas of all kinds instantaneously and inexpensively across national borders. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, internet has become an "enabler" of other human rights. Freedom on Internet ensures accountability from government. But misuse of cyber security policies like **cybercrime volunteer programmes** can affect the freedom enjoyed by people demanding accountability from the government. Internet Freedom Foundation(IFF), a digital rights group has said that the programme enables a culture of surveillance. The IFF also mentions that the programme could create a potential social distrust by encouraging civilians to report the online activities of other citizens. Also, there is no information available on how the Ministry will ensure that the program is not misused to extract misguided personal or political vendettas.

In 2019, Facebook-owned WhatsApp had confirmed use of **Pegasus** to target journalists and human right activists in India. In that case it was alleged that the NSO Group targeted around 1,400 WhatsApp users with Pegasus. Among those then targeted in India were several human rights activists and lawyers working in tribal areas, an **Elgar Parishad case** accused, a **Bhima Koregaon case lawyer** and others. In 2021 also, a global collaborative investigative effort, titled the Pegasus project, revealed that **Pegasus spyware** targeted over **300 mobile phone numbers** in India. As per reports, at least 40 journalists, Cabinet Ministers, and holders of constitutional positions were possibly subjected to surveillance. Pegasus shows that any country that can afford a few thousand dollars can hack the smartphones of important government functionaries. Hence, the need for a governance framework covering surveillance and information operations is necessary for national security. In a constitutional democracy like India which is also a signatory to the **International Covenant on Civil and Political Rights** as well as the **Universal Declaration of Human Rights**, there ought to be a certain basic understanding that regulation of the internet or internet-based services by governments have to respect basic human rights standards.

G. Defence Cyber Agency (DCA)

It is a **tri-service command** of the Indian Armed Forces. Headquartered in New Delhi, the agency is tasked with handling cyber security threats. It is a move to boost capabilities to fight against hackers, especially those coming from China and Pakistan. The DCA draws personnel from all three branches of the Armed Forces. The head of the DCA is an **officer of two-star rank**, and reports to the Chairman of the Chiefs of Staff Committee (CoSC) through the Integrated Defence Staff (IDS)

The **Indian Armed forces** have also taken steps for ensuring cyber security. **Network for Spectrum - Optical Fibre project** is a pan India network which has the requisite bandwidth for broadband connectivity across the country and is used exclusively by defence forces. The NFS has boosted the communication capabilities of defence forces in a major way by enhancing national operational preparedness, connecting critical defence locations securely and providing real-time connectivity in the highest battlefield of the world.

9.8. GLOBAL PRACTICES

USA has a **separate cyber command centre** which has the primary role of countering all adverse cyber activities which affect the country. United States Cyber Command (**USCYBERCOM**) is one of the eleven unified commands of the United States' Department of Defence (DoD). It unifies the direction of cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber expertise. "**Five Eyes**" is a coalition for joint cooperation in cyber intelligence sharing. It is an alliance of the United States, Australia, Canada, New Zealand and the UK. However, in recent years, many documents have revealed that the alliance has been spying on foreign nationals by circumventing the national laws on spying.

The **Israel Defence Force** (IDF) has created two elite units for cyber warfare viz. C4I (Command, Control, Communications, Computers and Intelligence) and Military Intelligence. The Israel government has actively sought out **private sector**

institutions and the civil society to create a wide network of cyber security experts. The National Information Security Authority was established in 2002, which is responsible for **preventing cyber-attacks against critical infrastructure**. Israel National Cyber Bureau (INCB), created in 2012, has been instrumental in creating a national cyber defence policy, partnerships with the private sector, and linking domestic and international cyber defence players. Israel also actively promotes cyber security start-ups.

Paris Call for Trust and Security in Cyberspace

The 'Paris Call' is a statement of consensus related to the growing concerns about cyber threats. It is a set of common principles agreed upon by like-minded countries, private sector entities and international civil society organizations. It was adopted at the UNESCO **Internet Governance Forum** (IGF) meeting convened in Paris. It was announced on the 12th November, 2018. The Paris Call includes nine goals within a broad framework of three themes viz. **An inclusive regulatory process** to gather the existing **cyber norm initiatives** in a single document and set out a framework for further negotiations. By doing this, the Paris Call aims to prevent fragmentation of norms. Involve the private sector within the cyber-security framework. Adopt a multi-stakeholder approach comprising of governments, NGOs, corporate houses to improve collaboration on matters related to cyberspace. **International Law and State sovereignty** to ensure that the regulation of cyberspace is carried out within the framework of the UN Charter and international humanitarian law in a coordinated manner. Appealed for preventing illegal and immoral interventions in national elections of countries. **Protection of humans and infrastructure** to protect individuals and critical infrastructure from any danger. Include the industries and civil society groups in promoting 'cyber hygiene' (everyday good practices for protecting the data and ensuring safety).

The call is non-binding. But the countries agreed on a number of key principles, such as importance of a peaceful cyberspace; relevance of international law and responsible behaviour by governments; and threat posed by malicious cyber activities. **'Paris Call'** has recognised that cyber threats are one of the greatest threats to the security of a country. It stresses on the benefits of a peaceful cyberspace, the importance of international humanitarian law and responsible behaviour by governments. It stresses the value of international cooperation and collectively addressing the threat of cyber-attacks.

9.9. WHAT MORE CAN BE DONE?

At a personal level, our devices should be protected by **passwords** and there should be **restricted access to sensitive data** on our devices. We must install antivirus software, personal firewalls and keep them updated. On notice of a suspicious process running on the machine, the internet connection must be turned off immediately so as to stop the cyber-attack in its early stages before it has the chance to finish the illegal routine. **Regular data backup** can be a solution to ransomware as the data backup will already be stored somewhere else, thus it will act as a deterrence against the blackmailers who are asking for ransom in return of unlocking the precious data. Using the knowledge gained from actual attacks that have already taken place, an effective and robust defence system can be built so as to avoid such incidents recurring in the future. For example, **PMGDISHA** (Pradhan Mantri Gramin Digital Saksharta Abhiyaan) is a step in the right direction as it promotes digital literacy in the rural masses.

At the national level, separate Indian IT service and cyber security courses can be started. The idea of a National Cyber Registry "**as a repository of IT professionals**" should be implemented. Government should also hire the best talent who are highly skilled by paying them market competitive remuneration so as to deal with cyber security issues in the most optimum way. Need of the hour for Indian government is to develop **core cyber security skills in youth, data integrity and data security awareness** while also setting

stringent cyber security standards to protect banks and financial institutions from cyber-attacks. The government should provide adequate funding for creating an indigenous electronics manufacturing ecosystem. **Research** should also focus on using **Artificial Intelligence** (AI) and **modern technology** for predicting in advance and accurately identifying attacks on cyber infrastructure so as to create a full proof cyber architecture. India's legal system too needs to be upgraded towards enhanced cyber laws as its present form is still dwelling on the IT Act, 2000 which is unable to cover the holistic issues in a field that is changing every day. The **cyber security measures** must adapt to keep pace and match the changing cyber risks and dynamics otherwise they will become ineffective overtime. Currently, organizations scram to keep their cyber security up-to-date; i.e., they "adapt" to changing requirements.

Experts are of the opinion that state cyber security framework should be envisaged in P-P-P model. Government should partner with the **private sector and academia** to strengthen cyber security posture of the state. Information security policies & practices should be mandated for government functionaries & its service providers. Security audits of all government websites, applications before hosting and publishing, should adhere to international standards. Government also needs to ensure that ISPs operating in the state deploy cyber security plans in line with state cyber security policy. Cyber security drills should be carried out under the supervision of CERT. Concept of air gapping which isolates the critical infrastructures from the internet also can be undertaken. Real-time intelligence, staff and infrastructure is required who can protect our cyber architecture round the clock for preventing and containing cyber-attacks. With the growing use of **online space and fast changing technology,** it is imperative for the authorities and citizens alike to step up their efforts in preventing the cyber-attacks which has a direct impact on our national security.

A **proper data protection law** with an effective enforcement mechanism would ensure recognition for India as a trustworthy global destination for data-based businesses and privacy-conscious consumers while also protecting the **Right to Privacy of the people in India**. Therefore, India should also make a proper data protection law along the lines of the EU's General Data Protection Regulation and the **US CLOUD Act**. The Centre had constituted the **BN Srikrishna Committee** (2017) to identify "key data protection issues" and suggest a draft data protection Bill. The **committee recommendations** are as shown in the figure. **Data localisation** norms also need to be promoted. Data localization is the act of storing data on any device that is physically present within the borders of a specific country where the data was generated. It is necessary for India because of securing citizen's data, data privacy, data sovereignty, national security, and economic development of the country. Thus, the government needs to take steps in the **promotion of data protection** and there is an urgent need to have an integrated, long-term strategy for policy creation for data localisation. RBI in 2018 had come up with guidelines for storage of customer data in India and has so far (till 2021) barred three foreign card payment network companies (Mastercard, American Express and Diners Club) from taking new customers on board, over its non-compliance.

BN Srikrishna Committee Report on Data Protection

The ten-member committee headed by Justice Srikrishna was tasked with studying and identifying key data protection issues and recommend methods for addressing them. The committee presented a draft data protection bill with the important provisions such as **'Individual Consent'** as a centrepiece of data sharing, awarding rights to users, imposing obligations on data fiduciaries (all those entities, including the State, which determined purpose and means of data processing). The Data Protection Bill also called for privacy by design on part of data processors, and defined terms like consent, data breach, sensitive data, etc. It also recommends **'Right to be forgotten'** in order to enable individuals to limit, delink, delete, or correct the disclosure of personal information on the internet that is misleading, embarrassing, irrelevant, or anachronistic. Creation of a **Data Protection Authority (DPA)** as an independent regulatory body responsible for the enforcement and effective implementation of the law. The law

would cover **processing of personal data** by both public and private entities. The Bill proposed that **critical personal data** of Indian citizens should be processed in centres located within the country. **Sensitive personal data** includes passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. The Bill also laid out provisions on **data storage**, making it **mandatory** for a copy of personal data to be **stored in India**. **Penalties** could be imposed for **violations of the data protection law**. The Committee had suggested a penalty of Rs. 15 crore or 4% of the total worldwide turnover of any data collection/processing entity, for violating provisions. Failure to take prompt action on a data security breach can attract up to Rs. 5 crore or 2% of turnover as a penalty. The penalties paid by violating entities would be deposited to a Data Protection Fund, which would, among other purposes, finance the functioning of the Data Protection Authority.

Though the draft bill addressed various issues plaguing the data ecosystem in India, it fell short on key principles that are at the core of a robust data protection framework. The Bill proposed that personal data of individuals could be processed for the exercise of any function of the state. This could be done **without the consent of the individual** as long as it was to provide a service or benefit to the individual. This is directly counter to the articulation of informed consent as central to informational privacy in the Puttaswamy judgment, 2017. Another key subject missing from the draft bill was the **reform of surveillance laws**. There is very little **legislative and judicial oversight on surveillance activities** carried out in India. As proposed by the Bill, requiring all businesses to store data within India, without any reform of surveillance governance, could pose even bigger privacy issues in the future.

Q. Data security has assumed significant importance in the digitized world due to rising cyber-crimes. The Justice B. N. Srikrishna Committee Report addresses issues related to data security. What, in your view, are the strengths and weaknesses of the Report relating to the protection of personal data in cyberspace? **(UPSC 2018)**

Further, **Gulshan Rai Committee recommendations** can be implemented by linking Indian Cyber Crime Coordination Centre to **NATGRID** and **CCTNS** (Crime and Criminal Tracking Network System) to deal with cybercrimes. A dedicated **cyber doctrine** to be undertaken at the time of a cyber-attack, must also be formed. The government must also think about **reducing the dependence on foreign servers** by creating one dedicated secure gateway for all government communication. The state governments should be sensitized for setting up **cyber forensic laboratories**. Central government can also take steps to spread awareness about cybercrimes, issue of alerts/advisories, capacity building/training of law enforcement personnel/ prosecutors/ judicial officers, improving cyber forensics facilities etc. to prevent such crimes and to speed up investigation. Cyber security awareness campaigns on the lines of 'RBI kehta hai' can also be taken up.

Crime and Criminal Tracking Network and Systems (CCTNS) is a mission mode project under the National e-Governance Plan (NeGP) of Government of India. CCTNS aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of policing. By adopting the principles of e-Governance and creation of a nationwide networking infrastructure, it aims at evolution of IT-enabled-state-of-the-art tracking system for 'investigation of crime and detection of criminals'.

National Intelligence Grid (NATGRID) is conceived to be an intelligence sharing network that collates data from the standalone databases of the various agencies and ministries of the Indian government. It is a counter terrorism measure that is expected to **collect and collate 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. This combined data shall be made available to 11 central agencies. As per news reports in September 2021, the Prime Minister is expected to launch NATGRID in a short time.

Lack of a single apex body is a major concern in dealing with cyber security issues. Currently, there are over **36 different central bodies** to look into cyber issues, each with a different reporting structure. Further, each state has a separate CERT. This is unlike that of other countries like US, UK and Singapore who have a unified body. India also suffers from inadequate cyber warfare apparatus in a world where offensive and defensive capabilities have emerged as the 5th domain of warfare. This is particularly crucial given the recent state backed massive cyber-attack faced by Australia allegedly planned by China in 2020. In fact, special focus is needed due to the asymmetric nature of cyber warfare. Experts believe that India needs to make a proper assessment of an offensive cyber doctrine for deterrence by exploring the prospects of acquiring **'cyber-weapons'** to do enormous damage to the adversary's networks. This concept of 'active cyber defence' is generally being adopted to address new challenges. There must be enhanced cooperation among nations and reaffirmed global call to action for all United Nations member nations to not attack the core of the Internet even when in a state of war. According to United States' military doctrine, Offensive Cyber Operations (OCOs) are understood to be operations that are "intended to project power by application of force in or through cyberspace.

Internet today is becoming a necessity for all citizens. However, this right to internet should also be subjected to certain limitations. For instance, provision of free wi-fi hotspots in military areas, honey trapping of military personnel using dating apps and websites, etc. have to be examined from

Should India Develop Cyber-Offensive Capabilities?

The uneasy reality of contemporary world is that the threat of war is not just limited to the conventional level of land, water and air. **Modern wars** have **proliferated into cyber space** and threat of information manipulation and cyber espionage have become a reality. In such a scenario only cyber defence is not enough. **Risks of information warfare** are **increasing** due to fast changing cyber threat landscape, rapid technological developments such as cloud computing, Artificial Intelligence (AI), Internet of Things (IoT), 5G, data protection/privacy and misuse of social media platforms, international cooperation on cybercrime & cyber terrorism, and so on. With the rise in cyber capabilities of neighbouring countries, India must be ready for any kind of offence. With cyber-offence capabilities in place, India will have geo-political advantage of using information warfare in its favour. Due to cyber-offence capabilities of a nation, other countries fear of carrying full-fledged war due to vulnerability of their critical infrastructure to any cyber-attack. It acts as **psychological deterrent** for other nations. Example - China is seen as power with high cyber-offence capabilities. Recently, issues with China has deepened with border skirmishes. Many of the cyber-attacks that India faces can be attributed back to China, as highlighted in a recent report to the National Security Council Secretariat. India needs to develop cyber-offence capabilities in order to counter and balance China.

Utility of **offensive defense strategy** is being increasingly accepted among the experts and offensive cyber capability is necesarry to give teeth to such a strategy. However, without cyber-infrastructure in place, cyber-offensive capabilities cannot be developed. What India needs is an aggressive **investment** in developing cyber-infrastructure. In order to keep up with the rapid pace of development in the cyber space, there is a need to invest more in emerging technologies like quantum computing, artificial intelligence (AI) etc. Also, broad policy initiatives are required to attract and retain talent in the indigenous cyber industry. Moreover, it is an imperative for the government to **partner with the industry and academia** to promote and encourage a robust ecosystem of ethical hacking. It will help us in not only identifying our vulnerabilities but also build foundation for our cyber offensive. There is a need to support and grow domestic cyber capabilities by working with cyber-defence industries and entrepreneurs. India is still depending on international private players for cyber security tools; we need to change it. More research needs to be done to understand the cyber capabilities of each country, how each country plans to integrate these capabilities into their national security strategies, how cyber capabilities could play into escalation or conflict in the region, and how cyber-enabled escalation or conflict could be managed. Cyber-sector demands highly skilled human resources. Efforts must be made to enhance the quality of human resource & create a **cadre of skilled professionals** in cyber domain. Industry must train young minds to be ready for any kind of information warfare.

a security point of view. It is possible to provide internet access to all ranks with suitable security instructions and a monitoring mechanism without impinging on privacy. Technology can be leveraged to improve security, something which is a necessity as far as Army is concerned. Cyber security needs to be given the impetus required to safeguard us from cyber threats. The process of providing government emails has already commenced. Army can fast track this process to ensure that all authorised users are provided secure government email, which in turn would become the primary mode of communication outside of the Army Intranet. It will enable official communications to move away from Gmail, Yahoo Mail etc.

The **Budapest Convention** of 2004 (The Convention on Cybercrime) is the first international treaty dealing with cybercrimes. Cyber experts believe that **India should consider signing the treaty** for effective international collaborations as we need to secure our computing environment with latest tools, patches, updates in a timely manner with the learnings gained from the best practices around the world. Promoting global cooperation in the area of cybersecurity is the need of the hour otherwise overt cyberwarfare will be a reality one day. Another initiative is the **Tallinn Manual**, which is an academic study on how international law applies to cyber conflicts and cyber warfare. The Tallinn Manual is neither a binding document, nor universally considered to be the definitive expression of cyber security norms. Yet, it is a valuable resource to identify rules where India's interests in cyber space demand interpretations that depart from western interpretations tailored to serve western interests. It can help India to object against the application of a rule at odds with our national security interests.

The government should adopt the **BIS Industrial Cybersecurity Standards**. The government also needs robust infrastructure, processes and audit system to strengthen cybersecurity. India can take examples from the North American Electric Reliability Critical Infrastructure Protection (NERC) policy. The policy could serve as a guide to the power sector companies and help in securing their operational technology (OT) networks. India so far has protected the critical networks like the sensitive Aadhaar ecosystem, the core banking systems etc. To strengthen it further, India can release a new cybersecurity policy addressing wider challenges. Apart from that, Ministries and Departments **need better budgetary allocations** for cybersecurity. National cybersecurity Coordinator must be strengthened to bring about much-needed synergy among various institutions and work out a coordinated approach to cybersecurity.

21st century India will be a **knowledge economy** and it would be facilitated through digital medium. Thus, it becomes a priority for all the stakeholders-government, private players, consumers, service providers and ordinary citizens to play their part to create a safe and secure cyber ecosystem. Cyber security is a challenge for nation's security as well as its growth and needs to be addressed with adequate attention. India is on the path of development and transforming into a **New Digital India**, for which it should take necessary measures to deal with cybersecurity challenges it is faced with. In the past it has been seen that various vulnerabilities have time and again caused economic and other losses, but since the creation of agencies like CERT etc. the defensive structure of India against cyber-threats has become much stronger. Thus, the government should work on creating solutions for the various challenges which affects Indian cyberspace so as to provide safety, security and protection for its citizens who use the internet. One needs to build deep technology in cyberspace and new technologies such as artificial intelligence, Machine learning, and quantum computing, present new opportunities in this regard.

Q. Keeping in view India's internal security, analyse the impact of cross border cyber-attacks. Also discuss defensive measures against these sophisticated attacks.
(UPSC 2021)

Role of External State and Non-State Actors in Creating Internal Security Challenges

10.1. INTRODUTION

In **security terminology, external state actors** refers to legitimate national government or organizations such as, government agencies, diplomatic corps, military institutions etc., that have direct or indirect relation with the state. For example, if we consider security threats to India, Pakistan as a state, **its armed forces, its intelligence agency** (ISI) etc., could be called as external state actors. On the other hand, **non-state actors** are those entities/individuals/agencies/ organizations etc., which have **no tangible linkage** with the state institutions. These organizations **act independent of state.** However, there may not be a **water tight separation** between state and non-state actors and non-state actors may act as a **proxy** for the state actors. Examples of common non-state actors are Terrorist organizations, civil-society groups, organized crime networks etc. In case of India, **Lashkar-e-taiba, Jaish-e-Mohammad, D-company** etc., could be termed as non-state actors that pose a significant security threat. In 2021, NSA Mr. Ajit Doval, termed **Civil-Society Organizations** as the new frontier of war.

10.2. CHALLENGES POSED BY STATE ACTORS TO SECURITY

State actors may pose direct threat to sovereignty or integrity of the nation through aggressions across borders or usurping the national territory. For example, China's occupation of Indian land northwards of Upper Subansiri district in the North Eastern state of Arunachal Pradesh in the 1950s.

State actors may also indirectly pose a threat through **diplomatic aggression**, subverting national interest by influencing policy of other nations, for example, diplomatic corps of China aggressively oppose India's membership in the Nuclear Supplier's Group (**NSG**) and promoting non-state actors involved in illegal activities. For example, Pakistan's ISI actively funds drugs/arms trafficking rackets operating in India. There have been reports of foreign funded NGOs thwarting developmental projects as seen in the case of Kudankulam Nuclear power project.

We have read in detail about threat posed by China and Pakistan in chapter on Terrorism (Chapter 3), Militancy in Jammu and Kashmir (Chapter 5), Insurgency in North-East (Chapter 6) and Border Management (Chapter 11).

10.2.1. Taliban Regime in Afghanistan

On February 29, 2020, the United States and the Taliban signed a **peace agreement in Doha**, Qatar. The provisions of the deal include the withdrawal of all American and NATO troops from Afghanistan. The agreement called for an Initial reduction of its force level from 13,000 to 8,600 by July 2020, followed by a **full withdrawal within 14 months**. The United States also committed to closing five military bases within 135 days. On its part Taliban pledged to prevent Al-Qaeda or any other terrorist organization from operating in areas under Taliban control. Further the Doha pact called for talks between the Taliban and the then Afghan government. However, the then **Afghan government was not a party** to the deal and initially refused to agree for the release of 5,000

Taliban prisoners. The **intra-Afghan negotiations** did not begin as planned and underwent lot of hassles. Despite the peace agreement between the U.S. and the Taliban, there were continued violent attacks on the then Afghan government by the Taliban.

The subsequent developments after the withdrawal of US troops from Afghanistan have resulted in a takeover by Taliban. Even though Taliban regime has not gained recognition from any country as yet, it exercises complete control over the day-to-day affairs of Afghanistan. These developments in Afghanistan have significant consequences for India's interests in the region and its security as a whole. Taliban's takeover will for example, prove detrimental to India's development projects in Afghanistan. For example, the Indian built projects, including **the Zaranj-Delaram Highway and Salma Dam**, are already under the Taliban control and there is an uncertainty with regard to those projects which are under construction, including check dams, schools and urban projects. It will also have an adverse impact upon the on-going peace initiatives in the Jammu and Kashmir. Further Afghanistan is a part of the **golden crescent** and a hub for international drug trade. Money from this drug trade is used to support militants in Kashmir and other terrorist groups. Taliban takeover has increased the instability in Afghanistan resulting in more **proliferation of drugs** and narcotic substances in India from the area of golden crescent. Taliban's control over Afghanistan in the past too have proved itself to be detrimental to India's security interests. For example, Taliban's takeover of Afghanistan in the 1990's pushed a wave of insurgents into Jammu & Kashmir through Pakistan. As the new Taliban regime lacks the legitimate sources to raise revenues for running the country, it will naturally rely on illegitimate sources to raise funds. Hence, it is highly likely that the Taliban regime will resort to illegal drugs and arms trade to ensure a steady money supply. As per a report of a UN Monitoring group, Taliban derives **50% of its revenues from taxes on poppy** cultivation. Large syndicates of organized crimes are involved in operationalizing this trade, with non-state actors facilitating smuggling of drugs, other crimes and terrorism. This in turn will strengthen the nexus of organized crime, money laundering, terrorism and trafficking in the region.

The Soviet withdrawal in 1989, during the last phase of the cold war, left the Pakistani military with a **large surplus of Islamist fighters** that it had trained and armed. Islamabad thus, gained a strategic depth in Afghanistan by working in close coordination with the leadership of the Taliban. Pakistan has used its influence in Afghanistan to intensify the **insurgency in the Kashmir** Valley. The present situation with Taliban at the helm of affairs in Afghanistan runs a similar security risk for India in Jammu and Kashmir. Further, many recent raids by the National Investigation Agency point to an Al-Qaeda network in India. The spill over effect of Taliban's resurgence in Afghanistan, will also be seen in Iran as well as the Central Asia countries. These areas are likely to see a rapid increase in extremism and radicalization. It will thwart the developmental and connectivity initiatives, like International North South Transport Corridor (INSTC), TAPI gas pipeline etc., that India is pursuing in this strategic part of the world. More so, India has had poor relations with Taliban and have always recognized it as a terrorist organization. On the other hand, India had cordial relations with ex-President Ashraf Ghani. Thus, the change in power structure in Afghanistan will not be without diplomatic and political challenges for India. Further, trade through Afghanistan under a Taliban regime would be routed through Karachi and Gwadar. Thus, it has a possibility that the Indian investment (financial and diplomatic) in the Chabahar port, meant to circumvent Pakistan, may become unviable.

In light of these developments there is a need for India to take pro-active diplomatic and political initiatives. Not only India has to protect its security interests but also ensure peace and stability in the region as a whole. Also, it is imperative for India to protect the goodwill (soft power) it has gained in the hearts and minds of the people of Afghanistan over the year. For this, India should enhance engagement with all the stakeholders of Afghanistan including Taliban. India needs to change its earlier stand of not recognizing Taliban. India should also consider appointing a 'special envoy' dedicated to Afghan reconciliation. To be more effective, India should

shift from aid-diplomacy to increasing investment in the region to deepen its presence in the region by involving private players. India should broaden its engagements with likeminded countries such as Iran, Russia, and United States on Afghanistan's future and carve out areas of convergence. India should promote the key projects like International North-South Transport Corridor (INSTC) to counter Chinese presence in the region and to bring other countries in the big picture. India could bolster the **institutional capacity of India's counterterrorism apparatus,** by training and properly equipping new and current personnel, augmenting intelligence capabilities and inter-agency coordination for providing swift, actionable intelligence and using technology like Artificial Intelligence to **monitor social media** use by terrorist outfits.

Further, India must improve coordination and information exchange between domestic and international intelligence agencies. Full activation of **NATGRID** is important. Financial transactions of the illegal activities conducted by the Taliban must be monitored. This is needed to avoid incidents like IC-814 Kandahar hijacking. Operationalization of **CIBMS** (Comprehensive Integrated Border Management System) for better border management will prevent illegal infiltration/ migration from the porous and geographically wide borders. The National Security Council and the Cabinet Committee on security must formulate a **counter-strategic program** against security threats from Taliban. As the situation in Afghanistan worsens, it will be in India's best interest to plan for the worst and hope for the best being mindful of present realities and history.

10.3. NON-STATE ACTORS

Various non-state actors that are a threat to India's internal security such as drug cartels, trafficking organizations, illegal immigrants, CSOs etc., have been discussed in this chapter. Non-state actors other than those mentioned here are discussed comprehensively in other chapters of this book.

10.3.1. Drug Cartels as an Internal Security Challenge

A drug cartel or syndicate is a criminal organization which is involved in conducting drug trafficking operations. Drug trafficking cartels can be a loosely managed agreement among various drug traffickers and/or can also be a formalized commercial enterprise, for example, D-Company. India's precarious position between **'Golden Crescent'** and the **'Golden Triangle'** poses a significant threat to the internal security of India.

Drug syndicates have the potential to provide **huge funds** and **logistical support** to various violent non-state actors. Such cartels find ready support from nation-states inimical to India's interest. For example, ISI recruits a number of **'carriers'** in drug trafficking as their agents, providing them **legal immunity** in their own country in order to carry out their nefarious activities in India. Taliban's

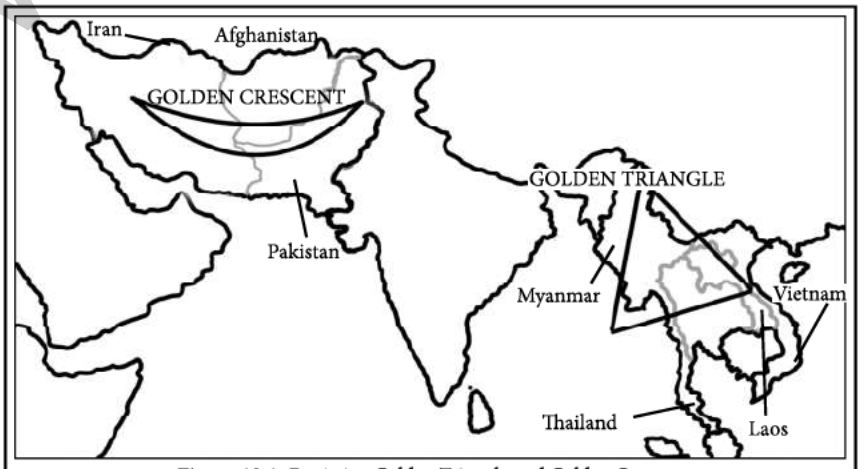


Figure 10.1: *Depicting Golden Triangle and Golden Crescent*

takeover of the civilian government in Afghanistan has the potential to further bolster the illegal drug trafficking activities in the region.

Increased production of opium in Afghanistan, greater domestic demand in India and alleged connivance of government/border officials have contributed towards increasing heroin trafficking, especially in the **Punjab sector**. Youth have been the targets and worst sufferers of the illicit drugs trade in Punjab. The demand for illicit narcotics drugs in Punjab is entirely met from outside the state through a supply of networks controlled by local, inter-state, and international criminal gangs. Punjab is both a **transit point and a market** for the drugs smuggled from the Golden Crescent (Afghanistan, Pakistan and Iran). While the Afghanistan heroin is smuggled from the porous Indo-Pak border, opium and poppy husk is smuggled from Rajasthan and Madhya Pradesh where poppy cultivation is legal. Charas and Hashish is smuggled from Himachal Pradesh besides the synthetic drugs. Drug units located on Himachal-Punjab borders produce ICE drugs. The 553-km-long International Border with Pakistan is porous at many places which also include local rivers where fencing is missing. Amritsar, Tarn Taran, Ferozepur and Fazilka districts sharing the border with Pakistan are part of the drug smuggling route which the Pakistan or Afghanistan based drug smugglers use to route their consignments.

The North-East region of the country too is becoming a hub for drug consumption and trafficking. Myanmar is one of the three countries that form the infamous **Golden Triangle –** a region where opium is produced in massive volume. According to United Nations Office on Drugs and Crime (UNODC), opium production has gone up in the Golden Triangle by 22 per cent.

Myanmar has totally failed in checking the growth of the drug trade within its borders, and this has resulted in an unbridled rise in production of all kinds of narcotics. China too faced a similar problem in the early 2000s, due to its 1997-km border with Myanmar but Beijing's shrewd political strategy ensured that the drug peddlers operating out of Myanmar shifted their base near Thailand. Northeast India , however, remains at high risk. Drugs including opium, heroin, methamphetamine and many more are smuggled from Myanmar into north-east. Arunachal Pradesh, Manipur, Mizoram, and Nagaland share their border with Myanmar. After entering India, the drug route bifurcates, with one channel moving northwards through **Moreh in Manipur** while the other moves southwards to enter **Champai in Mizoram.** Problem in North-East is compounded as Bangladesh is a transit country for drugs produced in the Golden Triangle and, to a much lesser degree, the Golden Crescent. Reports from the Indian Narcotics Control Bureau also indicate that heroin is smuggled from India to Bangladesh through the porous Indo-Bangladesh border. The smuggling in, diversion and abuse of pharmaceuticals originating from India is considered to be the largest drug problem in Bangladesh.

Also, it is apparent that international drug smugglers have been using **Nepal as a transit for smuggling** as it has been discovered that cocaine and heroin arrive in Nepal from Latin American countries such as Brazil and Peru. The cocaine and heroin are not sold in Nepal and instead exported to India, China, Thailand, Hong Kong, Singapore and Malaysia among other East Asian countries, stated by Narcotics Control Bureau.

Naxals exploit the 'Red corridor' for expanding their revenues and arms smuggling. Due to lack of infrastructural development, **they illicitly grow opium and cannabis** providing them ready money. Hence, areas affected by insurgency in the north eastern states and LWE are known to indulge in drug trafficking extensively. This is further substantiated by the **Narcotics Control Bureau's report** showing that largest seizures of drugs like opium, heroin, and cannabis took place in Red Corridor areas like Jharkhand, Andhra Pradesh and Bihar. Further, ports like Mundra, Vijayawada, Kochi etc., are becoming international transit hub for global drug cartels. In 2021 Narcotics Control Bureau seized 2.9Kg of heroin from a Zimbabwean national in the Kochi port. In September 2021, **3,000 Kg of drugs** were seized at Mundra Port in Gujrat. The traffickers, according to the authorities are making use of **technology and shell firms** to remain undetected.

Heroin, **Hashish** and other such commonly trafficked drugs pose not only an internal security

challenge but are also detrimental to the health of the consumers, posing a threat to the country's **'human security'**. Their addiction has negative socio-economic consequences for not only the consumers but for the family members as well. Financial loss, failing health, social stigma, involvement in criminal activities and diminished job opportunities are some of the negative consequences. Also, many drug cartels are alleged to have support from the corridors of power. Criminal proceeds raised from trafficking drugs goes in to election/political finding, thus, vitiating the process of free and fair elections.

India has formulated a **National Action Plan for Drug Demand Reduction (NAPDDR)** for 2018-2025. It aims at reduction of adverse consequences of drug abuse through a multi-pronged strategy involving education, de-addiction and rehabilitation of affected individuals and their families. Government is taking intensive preventive and interdiction efforts along known drug routes and strict surveillance and enforcement at import and export points. Training programmes are being conducted for various law enforcement officials to combat drug menace. **Border guarding forces, such as BSF, SSB and Coast Guard** are empowered to take action under **Narcotics Drugs and Psychotropic Substances (NDPS) Act**. India has signed MOUs, with friendly countries, to increase international cooperation for exchange of information and investigative agencies.

10.3.2. Human Trafficking Cartels as an Internal Security Challenge

Human trafficking can be defined as a criminal activity that exploits children, women, and men for a number of purposes, including sex and forced labour. South Asia, with India at its centre, is one of the fastest growing regions for human trafficking in the world. Thousands of people including women and children from deprived societies are lured to India's towns and cities and even sent abroad by traffickers. Human trafficking is not a standalone activity. It works in **cahoots with organized crime networks and terrorist organizations**. The proceeds from crime of human trafficking goes into **funding of anti-state activities.** Further, terrorist organizations have been known to indulge with human traffickers to buy the victims for **menial physical and sexual labour**. As per a **MoWCD report,** in 2016 alone 19,233 women and children were trafficked, with West Bengal seeing the highest number of victims. India serves as a major destination point for children and women trafficked from Bangladesh, Nepal and Sri Lanka. Simultaneously, India also plays a role as country of origin for trafficking victims. Kolkata, Bihar, Mumbai and North-East are the major transit points in India for trafficking of human beings. According to some reports 5 to 15 million girls and women are smuggled and trafficked every year from **Bangladesh to India and to the Middle East**. In the recent decades, **trafficking of women and human smuggling** have become quite rampant across the borders. The Centre for Women and Children Studies estimated that 27,000 Bangladeshis have been forced into prostitution in India. Poverty and hunger forces either the parents to sell the girls to traffickers or the girls themselves leave home and fall prey to traffickers.

Pandemic induced lockdown has aggravated the problem of Child trafficking. Government agencies have rescued almost 9,000 children from trafficking since the first lockdown. In other words, **21 children have been trafficked every day** over nearly 15 months. Children as young as 12 are trafficked across the States to work in factories in appalling conditions, where owners are turning to cheap labour to recoup their losses from the novel coronavirus pandemic. The Childline India helpline received 44 lakh distress calls over 10 months. Over a year, 2,000 children have arrived at its shelter homes and 800 rescued from hazardous working conditions. **Child marriages** are also rampant - over 10,000 cases were tracked between April and August 2020.

A child rights NGO, working with the Delhi Commission for Protection of Child Rights has highlighted the problem of **rampant child labour** during the pandemic. The children and their **families faced a loss of income and economic crisis**, causing families' reduced capacity to care for children in the long term thus pushing children towards unsafe labour making them vulnerable to trafficking. The pandemic has also caused, in some instances, **loss of parental care** due to death,

illness, or separation. Thereby placing children at heightened **risk for violence, neglect, or exploitation**. This is compounded by an erosion of 'checks' against child labour and child marriage provided by law, as well as the absence of scrutiny of schools and society. The increase in internet access in current times has also led to **cyber-trafficking**. A recent report by the **United Nations Office on Drugs and Crime** on the effects of the pandemic on trafficking mentions that the traffickers are taking advantage of the loss of livelihoods and the increasing amount of time spent online to entrap victims, including by advertising false jobs on social media.

According to some studies, **inter-state trafficking** cases are rampant from North-Eastern states to Uttar Pradesh, Madhya Pradesh, Punjab and Haryana. The victims are exploited for both bondage labour as well as sexual exploitation. Prostitution rackets, brothels etc., are not only an internal security challenge but also a risk to health and well-being of the society. Further the organized crime networks are intricately involved with the traffickers. While these organizations provide safe channels to the traffickers to traffic the victims, the victims in turn are used by the organized crime networks as mules to smuggle their contraband supplies. Majority of Internal Trafficking cases have a strong socio-economic linkage, as it is seen that 50% of the victim belong to Schedule Caste (SC) and up to 30% belong to OBCs. A former CM of Chhattisgarh, has stated that over 20,000 girls from the tribal regions are sold by traffickers in cities like Delhi, Bangalore, Chennai, Mumbai etc. in the last few years. Trafficking leaves a mental and emotional scar on the victim. International agencies and scholars have identified that human trafficking has long ranging **social, political, economic and human security** impacts. It affects the physical and mental aspect of an individual. Victims are at an increased risk of **Human Immunodeficiency Virus** (HIV) and **AIDS** . Also, it violates basic human rights of the victims like right to life, liberty and security. The proceeds of crime generated from human trafficking are also funnelled into **organized crime activities**. Thus, human trafficking is a serious challenge to a nation's internal security and also a threat to the country's human security.

Government has taken several initiatives to check the menace of trafficking. Trafficking in Human Beings or Persons is prohibited under the Constitution of India under Article 23 (1). The **Immoral Traffic (Prevention) Act, 1956 (ITPA)** is the premier legislation for prevention of trafficking for commercial sexual exploitation. **Criminal Law (amendment) Act** 2013 has come into force wherein Section 370 of the Indian Penal Code has been substituted with Section 370 and 370A IPC which provide for comprehensive measures to counter the menace of human trafficking including trafficking of children for exploitation in any form including physical exploitation or any form of sexual exploitation, slavery, servitude, or forced removal of organs. **Protection of Children from Sexual offences (POCSO) Act, 2012,** which has come into effect from 14th November, 2012 is a special law to protect children from sexual abuse and exploitation. It provides precise definitions for different forms of sexual abuse, including penetrative and non-penetrative sexual assault, sexual harassment. There are other specific legislations enacted relating to trafficking in women and children **Prohibition of Child Marriage Act, 2006**, Bonded Labour System (Abolition) Act, 1976, Child Labour (Prohibition and Regulation) Act, 1986, **Transplantation of Human Organs Act, 1994,** apart from specific Sections in the IPC, e.g., Sections 372 and 373 dealing with selling and buying of girls for the purpose of prostitution. State Governments have also enacted specific legislations to deal with the issue. (e.g., The Punjab Prevention of Human Smuggling Act, 2012)

The Government of India has **proposed the Trafficking in Persons (Prevention, Care and Rehabilitation) Bill, 2021.** This Bill aims to tackle all aspects of trafficking including the social and economic causes of the crime, punishment to traffickers, and the protection and rehabilitation of survivors. The bill defines exploitation to include the exploitation of the person for prostitution or other forms of sexual exploitation which includes pornography, forced labour, slavery, forced removal of organs, or illegal clinical drug trials. The bill extends beyond the protection of women and children as victims. It **now includes transgenders** as well as any person who may be a victim of

trafficking. The bill does away with the provision that a victim necessarily needs to be transported from one place to another to be defined as a victim of trafficking.

National Investigation Agency (**NIA**) shall act as the national **investigating** and coordinating **agency** responsible for the prevention and combating of trafficking in persons.The Punishment will be for a minimum of seven years period, which can go up to imprisonment of 10 years and a fine of Rs 5 lakh. However, in cases of the trafficking of more than one child, the penalty is life imprisonment. In certain cases, even the death penalty can be sought. There is provision for more severe penalties in case of aggravated offences, like the death of a victim.

There is no shortage of anti-trafficking policies in India but where the system is found **lacking is in the implementation** of the laws. The bill prescribes stringent laws, including the death penalty as an option in some cases. However, it is not proven that more stringent laws have any greater deterrent effect on crime. **Low conviction rates and lengthy trials** ail the criminal justice system. There were 140 acquittals and only 38 convictions in 2019, according to government data. This points to a failure of investigation and cannot be solved by the draft Bill's provision that accused traffickers must be presumed guilty unless they can prove the contrary. Further, trials can drag on for years, with victims sometimes withdrawing their complaints after being intimidated by traffickers.

To make the bill more effective, **proper case management** must be introduced to give meaning to the "fast track" courts and proper investigation of trafficking cases. To protect and rehabilitate the trafficked persons, the Bill has to include the **necessary checks and balances** against potential misuse of power by agencies. The bill also has to include **periodic reviews** of the law and its performance. Above all, the government has to **allocate adequate resources** for the effective implementation of the existing laws and the bill.

10.3.3. Fake Currency Rackets

Fake Indian Currency Notes (FICN) cartels are the organizations that operate by circulating **counterfeit** Indian currency. These organizations are supported by various state actors, like **ISI**, to fund the **terrorist activities**, organized **crime syndicates**, trafficking syndicates etc. These rackets beside being an internal security threat are also a cause of concern for the **financial security** of the country. Pakistan, Nepal, Bangladesh and Thailand are the main sources of Indian Fake Currency. The **modus operandi** of the groups is such that, big consignments of FICNs are brought to Bangladesh, Nepal from Pakistan through Gulf countries via air, and then smuggled into India through the porous borders. This illicit money is then channelled into funding of illegal activities like organized crime, terrorist activities, trafficking etc.

The Indian government has taken a slew of measures to counter the menace of fake currencies. A **coordination group** has been formed under the **Home Ministry** to coordinate the information and activities between the state forces and central agencies. Further, a **special cell** to counter terror funding and fake-currency has been formed under the **National Investigation Agency**. In addition, **RBI** from time to time takes adequate measures to improve the **security features** of the currency notes and to increase the **awareness** of the people to identify fake currencies. **FICN Coordination Group (FCORD)** has been formed by the Ministry of Home Affairs (MHA). It aims to share intelligence/information among the different security agencies of the state/centre to counter the problem of circulation of fake currency notes in the country. Also, **Terror Funding and Fake Currency Cell (TFFC)** is constituted under National Investigation Agency (NIA). Its aim is to investigate terror funding and fake currency cases.

10.3.4. Illegal Immigrants

Illegal migrants are the people who migrate into a country without an **official document** for their stay, or who stay in the country **post the expiry** of their valid **officially permit time**. India has been witnessing immigration since independence. People who have faced religious and political persecution, economic and social discrimination, cultural repression and curbs on personal freedom have made India their home. Of all kinds of migration, illegal migration has become the **most volatile and contentious issue** in Indian polity today because of the socio-political conflicts

it has brought in its wake. Illegal migrants from Bangladesh in particular is cause of concern for the security establishment of the country. Illegal migrants often are a cause of **ethnic trouble** in the country, as they widely **change the demography** of the host region. Such migrants, for example Rohingyas from Myanmar, are also a **direct threat for the security** of the country, as reported by various central intelligence/security agencies. The issue of migrants entering into the country illegally is also a recipe for **political instability** in the country. For example, the whole debate regarding **CAA/NRC** has more serious consequences in states like Assam, which are troubled with illegal migrants.

Apart from direct and indirect security threats as mentioned above, illegal migrants also pose various **governance challenges**, which puts pressure on the country's resources and manpower. For example, illegal migration in the country is directly proportional to an increasing pressure on resources like **land, jobs, government subsidies, education/health infrastructure** etc. Further, illegal migration, is directly linked to trafficking activities, prostitution, bondage labour and other illegal/illicit activities. Political factors have been one of the major reasons in forcing the Bangladeshi and Pakistani Hindus out of their country into India. Besides riots and war, discriminatory land laws were another region for immigration. At the same time, availability of land, better economic opportunities, education and health facilities and a similar cultural landscape have attracted these migrants to settle in India.

In Bangladesh, the already **discriminatory land laws** were further manipulated by vested interest groups and corrupt administrators to dispossess and alienate the Hindus from their own land and property. Religion has a particular effect in the case of the **Rohingya Crisis**. Growing population creates greater demands on resources such as land, food, energy, water and forest products, and their consequent overuse results in deterioration of quality. This process, in turn, encourages inequality in resource distribution among the rich and poor as the rich corner them and **deny the poor their share**. Industrialisation in India's neighbouring countries has not been able to keep pace with the growing labour force and as a result, the employment rate is declining. The working-age people who are unable to find jobs in the country look outside for employment opportunities. India shares a long and porous **international border with Bangladesh, Nepal and Bhutan.** The border traverses a range of natural and cultural landscapes, which pose a challenge to its effective management.

Illegal migration has resulted in **periodic clashes** between the citizens of India and migrants, leading to their loss of life and property, and thereby violating their **constitutional rights**. This has led to a feeling of dissatisfaction and anger among locals against immigrants and state for not taking any action against migrants. The rule of law and integrity of the country are undermined by the illegal migrants who are engaged in illegal and **anti-national activities**, such as entering the country fraudulently acquiring identity cards, exercising voting rights in India and resorting to **trans-border smuggling and other crimes**. The persistent attacks against the Muslims perceived as illegal migrants in Assam has given way to **radicalisation** within certain sections of the Muslim community. The formation of militant organisations, such as the **Muslim United Liberation Tigers of Assam** (MULTA) is a threat to national security.

Marginalization of the indigenous peoples in their own states as a result of demographic pressure exerted by immigrants had given rise to many protest movements in the region. An off-shoot of such movements is the emergence of many **insurgent groups** in the states like Tripura and Assam that create **internal security problems** for the Government. The influx of foreign nationals also create deep security concerns mainly in view of infiltration by the Islamic terrorists to foment trouble within India. Existence of many Islamic terrorist groups and collusive networks in Assam adds alarming dimension to **India's security problem**.

The first step towards addressing the issue of illegal migration is not to allow people to cross the international **border without authorisation**. For this purpose, border controls need to be made tighter to deter aliens from illegally crossing the borders. Despite experiencing continuous illegal migration, India's border had remained **poorly**

guarded. While some efforts for strengthening border controls along the border were envisaged, no concrete steps were taken to secure the border against illegal migration. **Augmenting the presence of the BSF** along the border to effectively man the border is an important step towards better border surveillance. **Border fencing** is a potential tool to prevent illegal migration. The international border shall be made secure against future infiltration by erection of physical barriers like barbed wire fencing and other obstacles at appropriate places. Further roads should be constructed to **facilitate patrolling by the security forces** and all effective measures should be undertaken to prevent infiltrators crossing or attempting to cross the international border.

The legislature enacted the **Foreigners Act, 1946**, by repealing the 1940 Act, conferring wide powers to deal with all foreigners. Apart from defining a 'foreigner' as a person who is not a citizen of India, it empowered the government to make provisions for prohibiting, regulating or restricting the entry of foreigners into India. The most important provision of the 1946 law, **which is still applicable** in all States and Union Territories, was that the **'burden of proof'** lies with the person, and not with the authorities. This has been upheld by **a Constitution Bench of the Supreme Court**.

In 1964, the government brought in **the Foreigners (Tribunals) Order**. The tribunal has the authority to decide whether a person is a foreigner within the ambit of the Foreigners Act, 1946. The tribunal, which has powers **similar to those of a civil court**, gives reasonable opportunity to the person alleged to be a foreigner to produce evidence in support of his case, before passing its order. In June of 2019, the Home Ministry made **certain amendments in the Foreigners (Tribunals) Order, 1964**. It was to **empower district magistrates in all States and Union Territories** to set up tribunals to decide whether a person staying illegally in India is a foreigner or not.

The **principle of non-refoulement** forms an essential protection under international human rights, refugee, humanitarian and customary law. It guarantees that no one should be returned to a country where they would face torture, cruel, inhuman or degrading treatment. This principle applies to all migrants at all times, irrespective of migration status. Under the International human rights law, the prohibition of refoulement is explicitly included in the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT) and the International Convention for the protection of All Persons from Enforced Disappearance (ICPPED). Also, the 1951 United Nations Refugee Convention, calls for the non-refoulement of the refugees. Government of India, in an affidavit submitted before the SC, said that it is **not a signatory to the 1951 United Nations Refugee Convention**, and hence is not obliged to adhere to the principle of non-refoulement.

Q. Cross-Border movement of insurgents is only one of the several security challenges facing the policing of the border in North-East India. Examine the various challenges currently emanating across the In-dia-Myanmar border. Also, discuss the steps to counter the challenges. **(UPSC 2019)**

10.3.5. Civil Society Organizations/NGOs

Civil Society Organization (CSO) is an umbrella term used for **non-profit non-government** groups their members come together to **achieve common share interests** and goals. While CSOs in India have performed yeoman service in diverse areas such as health, education, legal aid, drug rehabilitation etc., they have been **accused** by the critics to **instigate popular protest against government** initiatives leading the NSA to term them as a new frontier of war as recent as in November 2021. Some of the foreign-funded NGOs have been alleged to **propagate foreign propaganda** by stalling developmental projects. The negative impact on GDP growth is assessed to be 2%-3% per annum. E.g. The protests against Kudankulam nuclear plant

(being developed with Russia), protest against use GM seeds, Protest against POSCO and Vedanta plant in Orissa etc.

There is also issue of **mis-appropriation of funds by NGOs**. Sometimes, NGO has been floated to manage grants from the government for personal use. Enforcement Directorate had found that some NGOs which were working as front organizations for the banned Communist Party of India and were suspected to have funded Naxal operatives. Some NGOs work as **proxies of political parties to handle their unaccounted money** and campaign for their agenda. There have been reports of NGOs lobbying with parliamentarians and using the media to manipulate issues in their interest. Also, NGO have been found to be acting as conduits, **helping in money laundering**. According to an affidavit filed by CBI in the SC only 10% of all NGOs file annual income and expenditure statement. Many NGOs like Caruna Bal Vikas of Tamil Nadu, SCPPL etc., have been booked for violation of FCRA act.

NGOs have been found to be engaging **in anti-national activities** detrimental to national security. For example, ED have attached assets worth over 17 crores of Amnesty International (India) for involvement in money laundering activities. CSOs have seen to be stalling socio-economic developmental activities of the state by **channelling foreign funds to create local unrest**. For example, CSOs protesting against use of genetic engineering in agriculture or against nuclear power plants (Kudankulam) etc. According to an IB report the obstruction of government initiatives for socio-economic development by CSOs such as Greenpeace, ActionAid, Cordaid etc., have negatively impacted the GDP growth by 2-3%. CSOs like Greenpeace sparking protests against the coal fired plants, directly hinder the welfare objectives of the government. The energy produced from such plants is a direct enabler to uplift millions from poverty.

Key changes have been made in the Foreign Contributions Regulation Act (**FCRA**) in 2020 to better regulate the CSO/NGOs and prevent them from becoming a threat to country's internal security. The **public servants** (as defined under the Indian Penal Code) **are prohibited** from receiving foreign contributions. Foreign contributions once received **cannot be transferred** to any person or entity. **Aadhaar has been made mandatory** for all officials of recipient organisations. The government can now investigate the purpose and functioning of the recipient organisations. The amendment gives the Government power to suspend the registration certificate (which means that foreign contribution cannot be received/ utilised) of a person for up to 360 days (earlier 180 days). CSOs have been termed as the **new frontier of war by NSA** of India. This perception is far removed from their stated objectives of aiding in human and social development. To bridge the divide CSOs, need to work in tandem with state, follow financial transparency and align their work with the larger developmental objectives of the country.

Q. Analyse the multidimensional challenges posed by external state and non-state actors, to the internal security of India. Also discuss measures required to be taken to combat these threats.

(UPSC 2021)

Border Management

11.1. INTRODUCTION

Borders are the geographic extent of a country's **sovereignty, unity, and integrity**. Borders can be classified into three distinct sets viz. Land borders, Maritime borders, and Airspace borders. Border management is a multifaceted approach towards securing the borders in which along with the deployment of manpower and technology for the enhancement of border security, the regulation of legal and illegal immigration across the borders, ensuring the safe and secure cross border trade, and prevention of smuggling, trafficking of humans and cattle take place.

11.1.1. Historical Perspective

The evolution of boundaries in the Indian subcontinent has a long **historical and colonial legacy**. This has been a source of tension and conflict between the neighbors in the south Asian region. The outgoing colonial powers hastily drew the boundaries which left **uncertainties** with regards to boundaries between the newly formed entities of India, Pakistan, and Bangladesh (then East Pakistan). Along with these disputes, the **legacy border disputes** were also passed down to India by the colonial rulers, i.e., the border disputes with China, Nepal, and Sri Lanka.

11.1.2. Borders of India

The borders of India are quite complex having extreme geographical features and difficult terrains like Mountains (**Himalayan ranges in the north and north-east**), deserts in the North-west (**Thar desert**), swamps, marshes in the west and east (**Rann of Kutch and Sundarbans**), Tropical evergreen forests in the Northeast border states, and seas (the **Arabian Sea** and **Bay of Bengal** and the **Indian Ocean**) on the three sides of the Indian Peninsula.

India has a land border of **15,106 km** and a coastline of **7516.6 km**. All states except Madhya Pradesh, Chhattisgarh, Jharkhand, Telangana, and Haryana have an international border or a coastline. The **Department of Border Management**, under the **Ministry of Home Affairs (MHA)**, is tasked with securing most of India's borders, with some

Borders and Frontiers

Borders are **clear rigid** lines that **divide two political entities**. It marks the **limit of sovereignty** and jurisdiction of a State. Demarcation of border can be based on **natural features** like mountains, rivers etc. Borders can also be a result of mutually agreed **treaty** or a forced **imposition post a war**. For example: Border between USA and Mexico is marked by river Rio-Grande, border between India and Pakistan is defined by Radcliffe line.

Frontier is an **area extending beyond border**, acting as a **buffer zone** between two political entities. Unlike borders that are consequence of inward looking or centripetal forces, frontiers are result of **outward orientation** that results in creation of zone of interaction between two States. In modern world, more and more amorphous frontiers are being replaced by clearly defined borders. During medieval times, states were often separated by large expanses of forests without clear demarcation specifying limits of each state. Such forests were frontiers.

Border Management

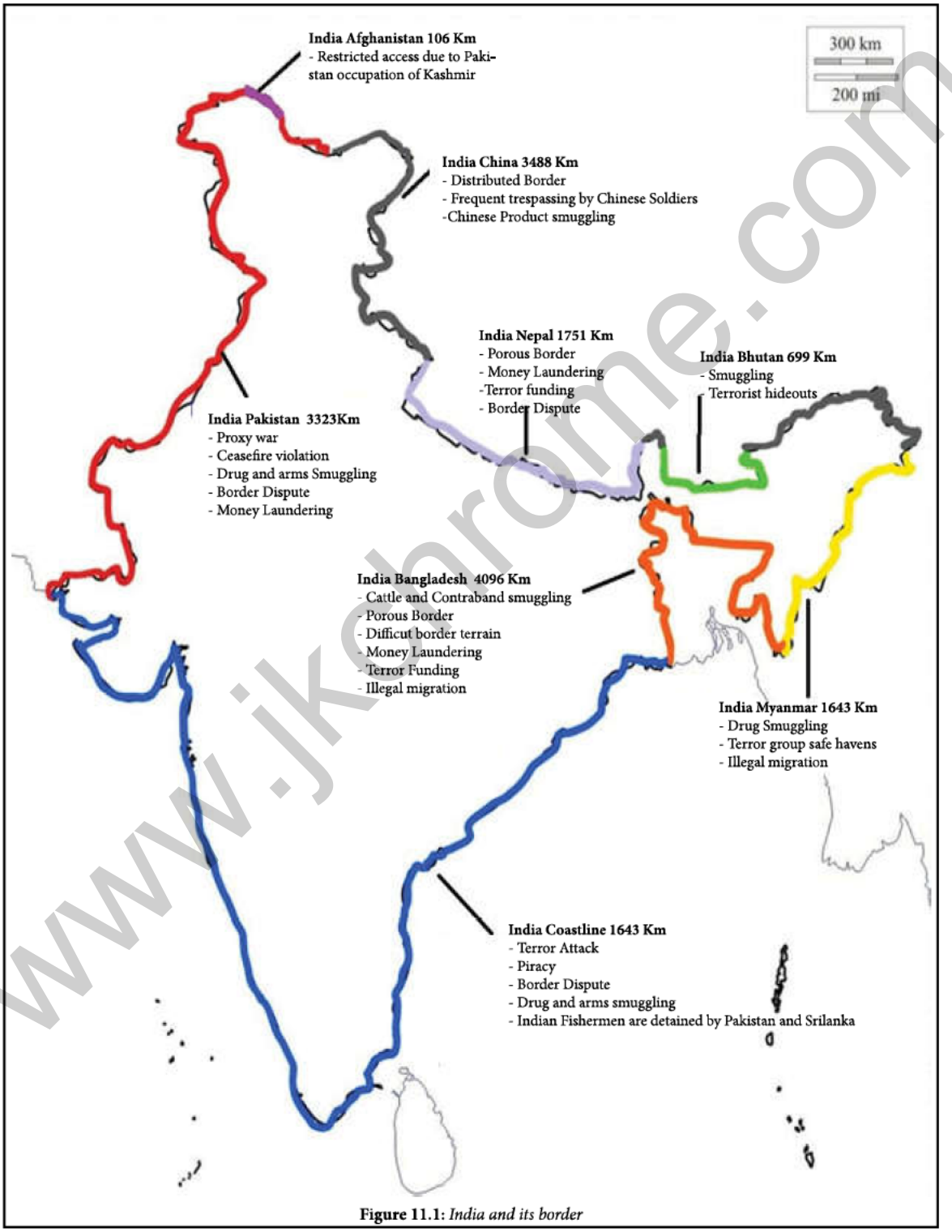


Figure 11.1: *India and its border*

of their key objectives are to prevent infiltrations, drug smuggling as well as facilitating trade and the safe movement of people.

11.2. COMMON CHALLENGES IN BORDER MANAGEMENT

Border Management in India is a **complex task** due to historical, geographical, political, social, and infrastructural factors. The most notable challenge is the absence of **properly demarcated** land and maritime borders. The colonial demarcation of border during the transfer of power/partition was done in a hurried and unscientific manner, without taking into economic, communication, ethnic, cultural or infrastructure considerations. Further, the geographical features and extreme nature of terrain also posed obstacles. The shifting sand dunes of the Thar desert shared between India and Pakistan led to undefined borders. The marshy, swampy and tidal flats regions of the Rann of Kutch led to the genesis of the **Sir Creek** dispute between India and Pakistan. The presence of Himalayan ranges leads to difficulty in border demarcation with China and Pakistan in the North. Dense tropical evergreen forests in the north east pose the challenge of border demarcation vis-à-vis India and Myanmar. Such geographical features lead to porous unmanned borders which is a huge threat. Border people are usually seen as **strategic assets** by security forces. They are instrumental in providing the **much-needed human intelligence**. For example, the information about the **occupation of forward posts at Kargil** was first given to the army by the **local herdsmen**. However, due to **threat to life and difficult living conditions** the border villages are **slowly depopulating**. It will deal a severe blow to the **human intelligence network** of the Indian security forces.

The local population residing in such border areas usually perform poorly on the socio-economic developmental indicators. Due to poor last mile connectivity, there is a lack of good governance as the benefits of government schemes often do not reach the border areas on time. As the border population lags behind in development parameters, sentiments of alienation and discrimination stems naturally in them. Also, due to poor economic/job opportunities, the locals in these regions are prone to radicalization and indoctrination by terrorist and extremist groups. These inimical state and non-state actors exploit the local residents for logistical support and shelter. These terrorist organizations are funded by hostile neighboring countries.

The other major challenge is the **infrastructure deficit** in the border regions. Due to difficult and **geographically fragile** terrain, the construction of roads, bridges, and other infrastructure is an expensive and time taking exercise. These projects mostly face time and cost overruns due to unforeseen circumstances and natural calamities like cloudbursts, landslides, avalanches, and flash floods. The border security forces face **shortages** of manpower, defense equipment and often depend on **redundant** technology for border security management. Also, the absence of physical and social infrastructure keeps the inhabitants of regions from tasting the fruits of growth and development happening in the country, thus, **preventing** them from joining the **mainstream**.

Another challenge is the issues faced by border security forces is **inadequate training** required for border security management. Under-trained and under manned border forces, are often unable to check cross-border smuggling of drugs, cattle, humans, artifacts, fake currency notes, etc. These shortcomings are a cause for serious lapses in border security management. These challenges are further **compounded** by meagre salaries, prolonged separation from family members, inadequate leaves, poor living conditions etc., which are a cause for depression/psychological problems in the security personnel, leading to incidents of suicides and fratricides. There is also a **lack of coordination** among multiple agencies like the Army, Border Security Force, paramilitary forces, Ministry of Defense, and Ministry of Home Affairs.

11.3. INDIA - PAKISTAN

India shares a 3323 km long and sensitive boundary with Pakistan. India's border with Pakistan is spread across extreme climatic conditions, ranging from the sub-zero temperature in the **Northern Himalayas** to the hot **Thar desert**. The India-Pakistan boundary is categorized under three different categories. The first is the **international boundary**, also known as the **'Radcliffe line'**. It is 2308 km long and stretches from Gujarat to parts of the Jammu district in Jammu and Kashmir which

is guarded by the Border Security Force (BSF). The second is the **line of control (LoC)**, or the Cease Fire Line, which came into existence after the 1948 and 1971 wars between India and Pakistan. This line is 776 km long and runs along with the districts of Jammu (some parts), Rajouri, Poonch, Baramulla, Kupwara, Kargil, and some portions of Leh. The third is the **actual ground position line (AGPL)**, which is 110 km long and extends from NJ 9842 to Indira Col in the North (Siachen Glacier). In the 1990s, India began to fence the massive border and by 2011 almost all of the border fencing, along J&K, Punjab, Rajasthan, and Gujarat was completed.

11.3.1. Issues of Border Management with Pakistan

Since the Partition of 1947, India has faced **proxy war** and **state-sponsored terrorism** by Pakistan. There have been attempts to destabilize India through infiltration and cross-border terrorism. Anti-India Jihadist groups in collusion with ISI, Pakistan's Intelligence agency, and Pakistan Armed forces constantly try to smuggle terrorists/arms to the Indian Side of LOC. There have been reports of terrorist training camps just on the other side of LoC. Firing and ceasefire violations from the Pakistani side have led to deaths of not only Indian soldiers but also of many innocent civilians. The diverse geographical physical features like hot sandy desert, swamps, and marshes, snow-capped mountains, and plains make border security a daunting task. Other issues include drug smuggling, fake currency circulation, arms trafficking, and money laundering. There are three areas of border dispute with Pakistan, one is the Kashmir region second is the Siachen glacier, and the Sir Creek region.

11.3.2. Kashmir Dispute

After independence, the state of Jammu and Kashmir acceded to India but Pakistan has always disputed it. After Jammu and Kashmir's accession to India, Pakistan tried to **infiltrate tribal warriors** into what was now **Indian territory**. The skirmish followed by a **UN intervention and subsequent ceasefire**, led to Pakistan illegally occupying the Indian territory. The region illegally occupied by Pakistan is called **PoK (Pakistan occupied Kashmir)** or **PoJK (Pakistan occupied Jammu and Kashmir).** It is controlled and administrated by Pakistan. It includes the region of **Gilgit Baltistan** and **Azad Kashmir**.

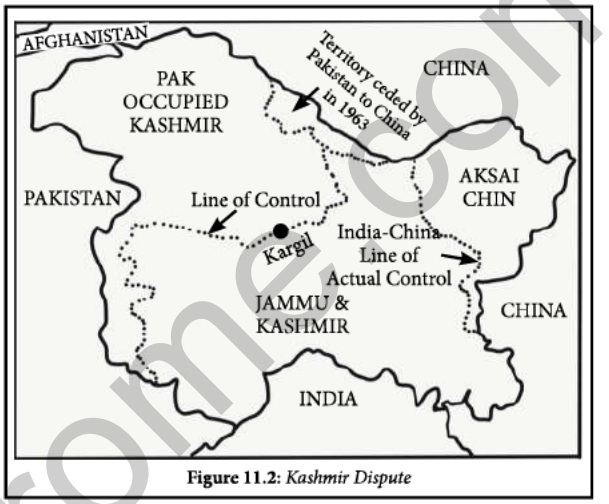


Figure 11.2: *Kashmir Dispute*

Shaksgam Valley: The region was part of PoK up to 1963. In 1963, Pakistan ceded the Shaksgam Valley to China.

11.3.3. Siachen Glacier Dispute

The dispute had its genesis in the Karachi ceasefire agreement of 1949. The agreement established the ceasefire line, the positions of the two militaries at the end of the 1947-1948 war, but did not delineate beyond grid reference point NJ 9842, which falls south of the Siachen glacier, towards the Chinese border. The agreement left it ambiguous as the terrain was inaccessible. In 1984, India got intel reports that Pakistan was planning to occupy the Siachen glacier. India launched **Operation Meghadoot** on 13 April 1984 and occupied strategic positions along the Saltoro ridge and since then the glacier is under the administrative control of India. Thus, since 1984 the Siachen glacier area has been the venue of a continuing military standoff between India and Pakistan. It is the highest battleground in the world. It led to the establishment of the **Actual ground position line (AGPL)** between India and Pakistan in the Siachen glacier.

11.3.4. Sir Creek Dispute

Sir Creek is a 96 km wide tidal estuary located on the border of India and Pakistan which opens up

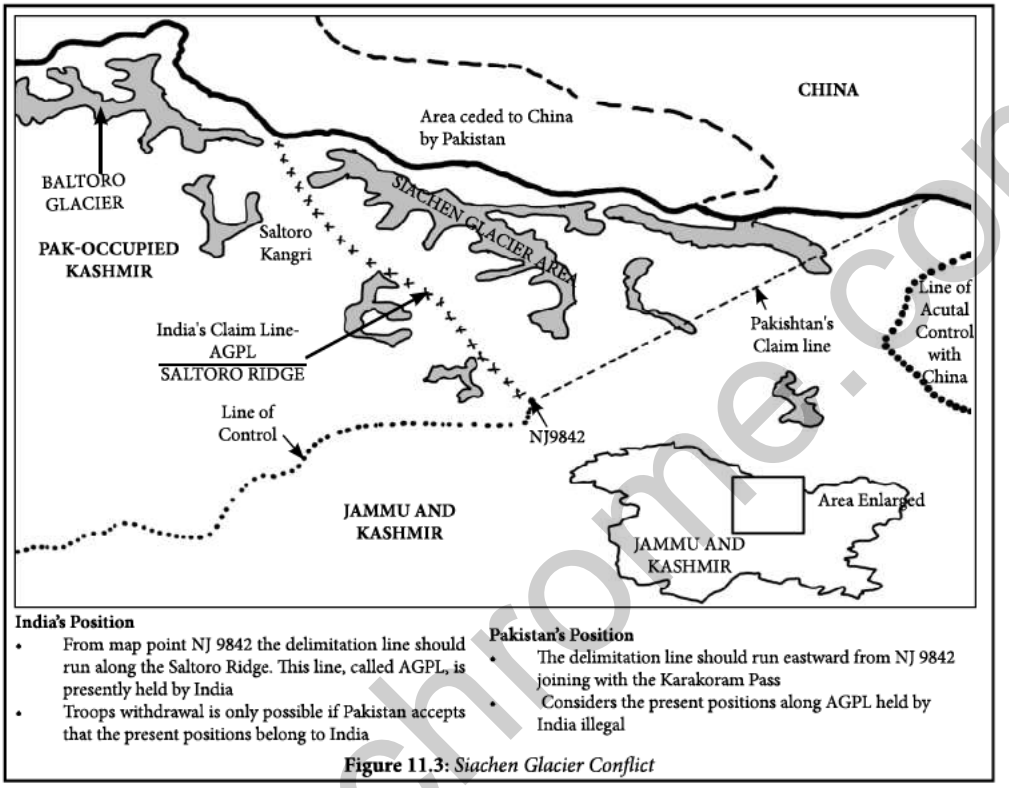


Figure 11.3: *Siachen Glacier Conflict*

into the Arabian Sea. It divides the state of Gujarat from the Sindh province of Pakistan. Pakistan claims the entire Sir Creek area based on a 1914 agreement signed between the government of Sindh and the then rulers of Kutch. However, India, on the basis of Thalweg principle, claims that the boundary lies mid-channel of Sir Creek, as depicted in a map in 1925 and implemented with pillars placed to mark the boundary. The area is of strategic importance as the forces of both countries sparred in this region in the 1965 war. Also, the area is rich fishing ground and could be a probable source of oil and gas. So, if one country agrees to the other's traditional position, then the former will end up losing a vast amount of Exclusive Economic Zone (EEZ) rich with gas and mineral deposits.

Thalweg principle: The thalweg principle, a part of international law, aims to resolve water boundary disputes. According to this doctrine, the boundary between two states divided by a flowing body of water may be drawn along the thalweg, which is the line of greatest depth of the channel.

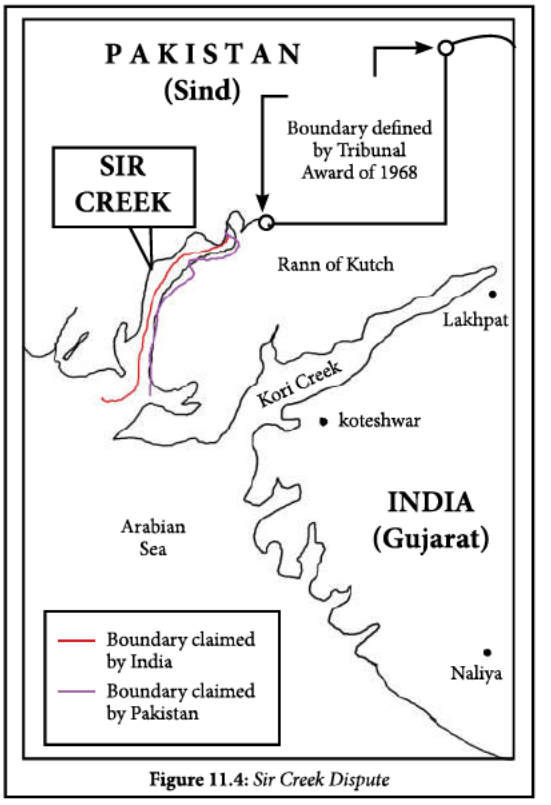


Figure 11.4: *Sir Creek Dispute*

11.3.5. Way Forward

India needs to open **diplomatic dialogue** with Pakistan to engage it in an amicable dispute resolution process. Also, India can use its economic prowess to create economic **interdependence** by means of bilateral trade. India can also leverage its **diplomatic influence** to stop Pakistan from sponsoring cross-border terrorism through forums like FATF, UN, etc. India should leverage technology for better management of the borders. For example, installing **smart fences**.

11.4. INDIA-CHINA BORDER

The India-China border also called **LAC (Line of Actual Control)** is divided into 3 segments: **The western sector, the Middle sector, and the Eastern sector**. The boundary dispute in the Western sector is with respect to the **Johnson Line** created by the British in the 1860s. extending up to the Kunlun Mountains, it included Aksai Chin in the then princely state of Jammu and Kashmir. While, India recognizes Johnson Line, China, does not recognize it and instead accepts McDonald's Line which puts Aksai Chin under its control.

In the Middle Sector (i.e., the Himachal Pradesh and Uttarakhand), the dispute is a minor one. Here LAC is the least controversial except for the precise alignment to be followed in the Barahoti plains. India and China have exchanged maps on which they broadly agree.

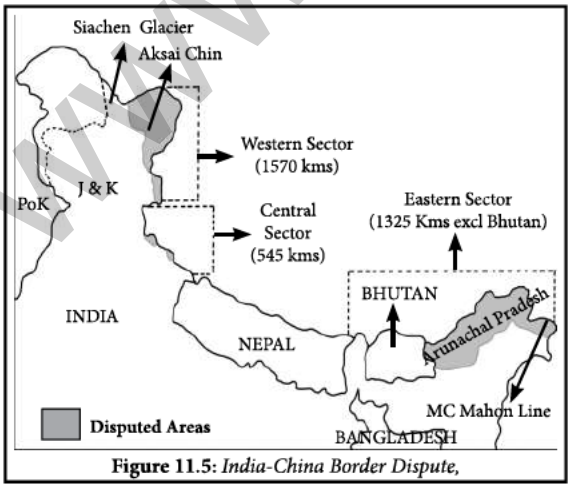


Figure 11.5: *India-China Border Dispute,*

The disputed boundary in the **Eastern Sector** (i.e., the **Arunachal Pradesh and Sikkim**) is over the **McMahon Line** (in **Arunachal Pradesh**) decided in 1914 in a meeting of representatives of **China, India,** and **Tibet** in **Shimla**. Though the Chinese representatives at the meeting initiated the agreement, but they subsequently refused to accept it. Arunachal Pradesh, which is a part of India, is also claimed by China as south Tibet.

11.4.1. Issues

Border dispute between the two country is the major roadblock in a stable bilateral relationship. Also, the unclear stand on the border is the source of sporadic trespassing of forces of both sides into the territory of other countries. In the year 2020, Galwan clash resulted in the killing of soldiers on both sides. Doklam standoff in 2017 was a result of illegal Chinese incursion into the trijunction area. The other major issue is the construction activity undertaken by both the countries along the border, which raises doubt over each countries intention, raising the issues of violation of sovereignty, thus, deepening the trust deficit. However, China has undertaken a large-scale effort to upgrade air, roads, and rail infrastructure, as well as surveillance capabilities near the border. To further complicate the issue, India's border is being guarded by multiple forces along the Indian border like **ITBP, Assam rifles, Special Frontier Force** as opposed to single **People Liberation Army (PLA)** on the Chinese side. This leads to a lack of intra-agency coordination hampering holistic border management. China is engaging itself in Building border villages. In the year 2020, satellite images showed 100-odd houses built on the land north of Arunachal Pradesh's Upper Subansiri district. The region was once a part of India. It was occupied by China in the late 1950s.

11.4. 2. Way Forward

India and China need to **clearly demarcate** the LAC by exchanging the border maps by engaging in bilateral dialogue. India could use multilateral platforms like **BRICS, SCO,** and **UN** to put pressure on China to resolve the border dispute on a priority basis. Until and unless the border dispute is resolved the relations between the two countries would suffer from mistrust and the bilateral relations would be a zero-sum game. Further, India needs to develop basic infrastructure along the India-China border

at par with China. So, in case of any exigency, India could easily deploy its troops and confront the threat. Also, the dispute between the two countries is consequential for other countries as well, as there could be no genuine Asian century without the resolution of border dispute between the two most influential/powerful countries in the region. According to many scholars and experts, China is not interested to resolve the border issue as it is **widely increasing its own infrastructure capacity** along the LAC. Once it creates the **asymmetry of border infrastructure vis-à-vis India**, in terms of defense and civil infrastructure it will no longer need to resolve the border dispute. This is in line with the known Chinese policy of hoodwinking its neighbors.

11.5. INDIA- BANGLADESH

India shares its longest land border with Bangladesh which includes West Bengal, Assam, Meghalaya, Tripura, and Mizoram. The entire stretch of the border consists of plain, river, marshes, hills, and jungle. The area is heavily populated, and at many stretches, the cultivation is carried out till the last inch of the border.

11.5.1. Issues

One of the biggest issues between the two countries is **Illegal migration**. Since the buildup to the 1971 war between India and Pakistan, millions of illegal Bangladeshi immigrants have poured into India. Another major issue is **Trafficking** which includes **humans, Cattle, FICN and other contrabands like drugs**. Along with above mention items, there is also rampant smuggling of arms, and other essential items such as sugar, salt, and diesel. Also, kidnapping, and thefts are quite rampant along with the India–Bangladesh border, which not only creates law and order problems but also creates a threat to national security.

Another notable issue is the use of India-Bangladesh border, being used to harbor insurgents by anti-India establishments like the **United Liberation Front of Assam (ULFA), The All-Tripura Tiger Force (ATTF), The National Liberation Front of Tripura (NLFT),** and the **National Democratic Front of Bodoland (NDFB)**. These insurgent outfits carry out attacks on Indian security forces and also **radicalize youths** to take up arms. Lastly, the border between the countries is **porous** as there is inadequate border fencing due to the difficult terrain like riverine areas, marshes, etc. accompanied by protests by the residing population who resist fencing as it curbs their movement across the border. Of late there have been several incidences of attacks on Hindu temples in Bangladesh and similar attacks on Bangladeshi immigrants in India. These incidents are a cause of concern as they have increased the distrust between the people residing on both side of the borders.

11.5.2. Way Forward

Bilateral diplomatic engagement is required to resolve the issue of illegal migration between India and Bangladesh. Sharing a **digital database** of its citizens will make it easier to track and extradite illegal migrants to their home country. **Border fencing** in Assam must be completed forthwith on a war footing, so as to plug the holes in the porous border management. The existing Border Security Force posts and the **BSF water wing** should be strengthened, as rivers like the Brahmaputra cannot be fenced. Also, India's technological advancement should be leveraged to install **smart borders and deploy drone-based surveillance**, in line of **CIBMS**, to counter illegal migration.

Comprehensive Integrated Border Management System (CIBMS): CIBMS is the integration of **manpower** (security forces), sensors and **command and control** to improve **situational awareness** and facilitate **quick response** to emerging situations. Virtual fencing, command and control and power management are important components of CIBMS. CIBMS functions to safeguard the **geographically hostile borders** in a smart/effective way by leveraging technology. **Thermal imager** indicates body heat signatures of any living being that moves towards Indian boundaries. Also, **night vision devices (NVDs), long range radars, battlefield surveillance radars**, etc., slightest of variations. **Analytical tools** identify suspicious movements and distinguish between man and animal from the shadow. **Motion sensors** in CIBMS have enhanced the efficiency of tracking the intruders and have also reduced the electricity bill associated with the floodlights, which were used for the same purpose.

BOLD-QIT: Border Electronically Dominated QRT Interception Technique (BOLD-QIT) is the project to install technical systems under the CIBMS, which enables BSF to equip Indo-Bangla borders with different kind of sensors in unfenced riverine area of Brahamputra and its tributaries.

BOLD-QIT covers the entire span of River Brahamputra with data network generated by Microwave communication, OFC Cables, DMR Communication, day and night surveillance Cameras and intrusion detection system. Leveraging these modern tools, security forces can timely thwart any possibility of illegal Cross Border Crossing/Crimes.

11.6. INDIA - NEPAL BORDER

India and Nepal have shared an open border since 1950 which have been an enabling factor in the **Roti-Beti** (employment-matrimonial) ties shared by the two countries. Its legal conception came up with the **Treaty of Peace and Friendship** that the two countries signed in 1950. The treaty provides citizens of both countries equal rights in matters of residence, acquisition of property, employment, and movement in each other's territory. Nepal's border lies across five Indian states viz. Uttarakhand, Uttar Pradesh, West Bihar, Sikkim, and Bengal. While open border has been a great facilitator of strong bilateral relations, however at the same time, it has given rise to many irritants and problems that raise serious concerns for India's internal security.

11.6.1. Issues

There has been credible evidence to prove that the Nepalese territory problem is **used by Pakistani Inter-Services Intelligence (ISI)** to carry out anti-India activities since the 1990s. As per WikiLeaks documents, it has been revealed that the ISI has created a number of terrorist fronts in Nepal and used them to **infiltrate terrorists and explosives** through the border to carry out terror attacks in India. The porous border between the two countries gives a **safe passage** to miscreants to carry out illegal activities such as **smuggling** of essential items and fake Indian currency, gun-running, drugs, and human and animal **trafficking**. Recently, the border dispute between the two countries had spiraled out of control. India and Nepal have a territorial dispute over the region of **Kalapani, Limpiyadhura,** and **Lipulekh** in the **Pithoragarh district of Uttarakhand**. Kalapani is a tri-junction point, where the Indian, Nepalese, and Chinese borders meet.

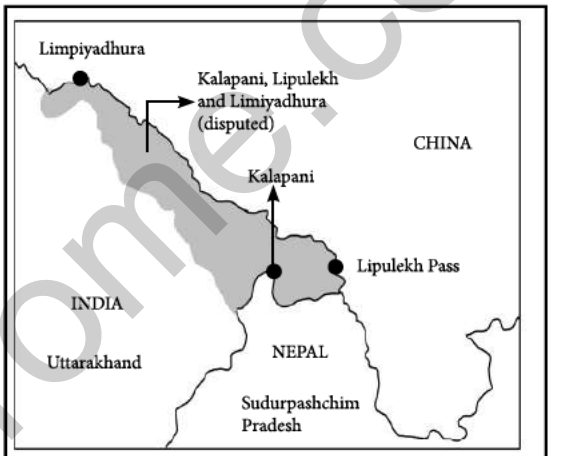


Figure 11.6: *Kalapani Dispute*

The disputes originate from the disagreement over the **interpretation of the Sagauli** Treaty which was signed in 1816 between the British East India Company and Nepal. It delimited the boundary of Nepal to the east of Maha Kali River in Nepal. India and Nepal have also had disputes over the issue of **compensation** of the Kosi dam. Also, there have been allegations of excesses, such as intimidation and coerced land grabbing by both sides along the disputed border. The disputed border has created dismay not only between the two countries but also among the local populations on both sides. Also, there is a rise in anti-India political sentiment in Nepal. Nepalese leaders often wage anti-India sentiments to display their nationalistic credentials. Further, **incidents like the 2015 blockade** on Indian borders restricting the supply of essentials like cooking gas, medicines etc., fares badly for the smooth bilateral relationship.

11.6.2. Way Forward

Nepal acts as a **buffer state** between India and China and has immense strategic relevance to India. So, India should try to resolve the **Kalapani dispute** amicably on a priority basis. Otherwise, this

discord between the two nations has the potential to disrupt the other aspects of their ties, especially in the domains of the **economy and cross-border security**. Further, it might give other stakeholders such as China an opportunity to interfere in the bilateral matter of the two countries. Also, India's engagement with Nepal has been episodic and crisis-driven, and not backed by the continuous human and material resources that our neighbor deserves. Furthermore, both countries are affected due to the misuse of the open borders by internal and external forces, the responsibility of border management and regulation depends on both. Therefore, both the nations need to iron out the issue amicably so that the cordial relations between the two neighbors are deepened.

11.7. INDIA - MYANMAR BORDER

India and Myanmar share a long **geographical** land border spread across 4 Indian states: Mizoram, Manipur, Nagaland, and Arunachal Pradesh, and maritime boundary in the Bay of Bengal. Frontiers of British India and Myanmar came into direct confrontation for the first time during the Anglo Burmese war of 1826. By the Government of India Act of 1935, Burma was severed off from India. After Independence, the boundary was demarcated in 1967 under an agreement signed by both countries. Even though the boundary is properly demarcated, there are a few pockets that are disputed.

11.7.1. Issues

The India-Myanmar border is characterized by **high mountains, deep river channels** together with lush humid forest. Such a terrain does not allow the construction of means of **transportation** and **communication**. The absence of these border guarding infrastructures adversely affects policing and allows insurgents to easily enter into Indian territory.

There is a **Free Movement Regime (FMR)** between the two countries. The FMR permits the tribes residing along the border to travel 16-km across the boundary without visa restrictions. While the FMR has helped the tribes continue to their age-old ties and practices, it has also become a cause of concern for the security forces as its provisions are exploited by the Indian insurgent groups to cross over to Myanmar unrestricted and establish safe-havens.

Also, since the start of the **insurgency** in the Northeast in the 1950s, the Naga, Mizo, Meitei, and Assamese insurgents groups have been **crossing over into Myanmar** to set up bases, where they have built safe heavens to recoup and launch offensives on Indian security forces, and sneak across the border to the hideouts when pursued by the Indian security forces.

Further, the border between the two countries also lies at the edge of the **"Golden Triangle"**, which facilitates the unrestricted illegal flows of **drugs into Indian territory**. The Golden Triangle is the area where the boundaries of Thailand, Laos, and Myanmar meet at the confluence of rivers **Ruak and Mekong**. Heroin is the main item of drug trafficking. The bulk of heroin enters India through the border town of **Moreh** in Manipur.

Moreover, the recent **Rohingya exodus** from Myanmar into neighboring countries including India has become a **security challenge**. These refugees not only create an economic burden on the host country but are also perceived as a threat to national security. Indian intelligence has claimed that some Pakistani-backed groups could enter as Rohingya refugees.

11.7.2. Way Forward

India should leverage forums like **BIMSTEC**, which can be used to discuss issues like illegal migration from neighboring countries and garner support and coordination from the members. This forum can help India to **engage Myanmar**, to find an amicable resolution to the current **humanitarian crisis**. Also, both countries are affected due to the misuse of the open borders by internal and external forces, the responsibility of border management and regulation depends on both. Further, India needs to enhance economic interdependence with Myanmar on a priority basis, because such economic partnership will help to boost border infrastructure and engage the youth by creating meaningful employment opportunities.

11.8. INDIA - BHUTAN BORDER

India shares a long border with Bhutan which spreads across states of Sikkim, West Bengal, Assam,

and Arunachal Pradesh. The basis for bilateral relations between India and Bhutan was formed by the **Indo-Bhutan Treaty of Peace and Friendship of 1949** and since then the relations between the countries have been cordial. The border between the two countries has been demarcated except along the tri-junction with China (**Doklam plateau**). Like Nepal, India's boundary with Bhutan is also an open boundary. The border between the two countries has largely been was peaceful except for a few sporadic incidents. As a responsible power, India should not only **refrain from interreference in domestic matters** of Bhutan but also should not even seem to be interfering in their internal matters.

11.8.1. Issues

There had been many insurgent groups that used Bhutan territory as a safe hideout such as the **Bodo liberation tiger (BLT), ULFA**, etc. These groups carried out illicit activities like extortion, assassinations, or attacks on Indian forces and then sneak into Bhutan to escape any action by the Indian Security forces. However, most of these groups have been wiped out by the **joint action of the security forces** of both countries. The other major issue between the two countries is the smuggling of goods like Bhutanese cannabis, liquor, and forest products, etc. Livestock, grocery items, and fruits are smuggled out of India to Bhutan

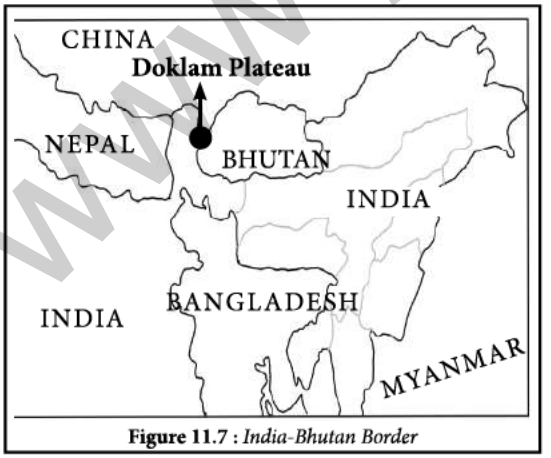


Figure 11.7 : *India-Bhutan Border*

11.8.2. Way Forward

Bhutan is of great strategic importance to India, as it acts as a buffer between India and China. Also, under the **Treaty of Peace and Friendship**, India is responsible to protect Bhutan from any external threat. So, it is important for India to immediately resolve the Doklam dispute between the three countries (i.e., India, Bhutan, and China) in its favor. As the Doklam is located close to the 'chicken neck corridor' of India **(Siliguri Corridor),** its access to China has the potential to jeopardize India's national security. Also, from an internal security perspective, the illicit establishment of camps by militant outfits in the dense jungles of south-east Bhutan is a cause of concern for both nations that need to be tackled.

11.9. ENSURING EFFECTIVE BORDER MANAGEMENT

One of the major issues facing the Border guarding forces is their **diversion to other roles** like election duty, or for providing security cover during major events. The border-guarding force should not be distracted from their principal task and deployed for other internal security duties. For eg-ITBP, a force specifically trained for India-China border should not be used in the Naxalite-infested areas.

It is felt that the responsibility for unsettled and disputed borders, such as the LoC in J&K and the LAC on the Indo-Tibetan border, should be that of the Indian Army while the BSF should be responsible for all settled borders. The border guarding forces should be aided by **satellites and drones**. 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 Organization with a two-way messaging system in all local languages.

Inter-Agency coordination also needs to be improved. So that better sharing of intelligence and information takes place among different agencies such as RAW, IB, Army, Coastal Police, Navy, etc. The border guarding forces need to be **modernized** on the lines of the National Army. Delays in procuring weapons should be avoided. Also, Defence Ministry should promote Make in India to indigenize weapons and equipment.

Further, border area management cannot be effective without **denying local support to**

militants. This can only happen when local population has **confidence in intention and capacity of the government**. Local population should feel that their interests are aligned with the interest of the nation and path of **violence** taken by militants is not only **futile** but also **counter-productive**. Administration in border areas should be strengthened by promoting grassroot **democracy**, encouraging **participation** of local population in decision making and devolving real power to the people. For areas under **Schedule 5 and 6**, respect should be given to traditional law and customs while also ensuring greater degree of autonomy. To **counter propaganda and radicalization**, government should use the power of digital and social media to dispel disinformation and misinformation. Creating **economic opportunities** in the border area through creation of infrastructure, promotion of industries and encouragement of the hospitality sector is very important to ensure that energy of youth is channeled in a productive direction. Closer co-operation between central security forces, state police force and local administration can help in perception management of the local population that security forces are there to protect them and not to suppress them. Moreover, government should take steps to **address** issues related to change in demographic profile and loss of local culture, language and customs under influence of outsiders in border areas that create a feeling of **'attack/assault' on culture**, sometimes driving people towards extremism and militancy.

Q. For effective border area management, discuss the steps required to be taken to deny local support to militants and also suggest ways to manage favourable perception among locals. **(UPSC 2020)**

Surgical strikes and Hot Pursuit

In recent years, Indian government has overtly ascribed to a **counter-insurgency (CI) strategy.** which involves actually crossing international borders to strike at anti-India insurgents. We often hear about Hot Pursuit and Surgical Strike in news and public debate forums. **Hot pursuit** means **chasing perpetrators** who have committed an unlawful act on a country's soil/territorial waters, even beyond its sovereign border. **Surgical strike** is a **precise attack** to damage/destroy a **legitimate military target** without causing damage to nearby civilian areas. This strategy is used against insurgents including those from the Northeast, who carry out hit-and-run raids taking advantage of their shelters in adjoining nations like Myanmar. Hot Pursuit was seen in action along the India-Myanmar border in 2015, during the pre-dawn 'surgical strike' by the Indian Army on two insurgent bases in western Myanmar's Sagaing division, across the Manupur and Nagaland sectors of the borders. The Hot Pursuit in Myanmar was conducted to neutralise the separatists (NSCN-K) who ambushed and killed 18 soldiers of the Indian army in Manipur. Later in September 2016, the Indian Army launched the biggest surgical strikes against terrorist camps in Pakistan occupied Kashmir, and destroyed terror launchpads along the Line of Control. The attacks were carried out in wake of the Jaish-e-Mohammed's attack on Uri base, killing 19 Indian soldiers.

Such actions have long lasting **strategic impacts**. For once, it displays the **military/armed capability** of the country. Hot Pursuit effectively projects the country's will and ability to defend its territory against all form of aggressions. As an instrument of **power projection**, such CI strategy may have **effective deterrence effect** on the minds of inimical interests.

It has a psychological impact on the minds of the preparators of terror and prevents them from committing acts of terror and breaching the sanctity of borders at will. At the same time it has a positive impact on the minds of the **citizens** as they feel safe with a **reinforced confidence** on the ability of the forces. Also, such a strategy is cost-effective as precision attacks are carried out on selected targets. It also keeps the number of civilian causalities to a minimum. Further, such strategy also has the effect of boosting the morale of the armed forces. Though, a suitable strategy there is a downside too. Excessive use of this strategy can lead to worsening of diplomatic relations between the two countries. Hence, it is advisable to **employ strategic restraint** when engaging in CI strategies like Hot Pursuit.

Q. The terms 'Hot Pursuit' and 'Surgical Strikes' are often used in connection with armed action against terrorist attacks. Discuss the strategic impact of such actions. **(UPSC 2016)**

11.10. COASTAL SECURITY

India has a 7,516 Km long coastline that includes 5,422 kilometers of coastline on the mainland and 2,094 kilometers on the islands. The coastline houses 13 major and more than 200 minor ports, along with 95 landing centers, and is increasingly facing security challenges from adversarial neighbors and non-state actors.

11.10.1. Security Concerns

India faces a number of security challenges along its coast ranging from terrorism, piracy, and border dispute, etc. The lack of security at the Indian seas has been exploited by the terrorist to launch attacks on India like the **Mumbai blast** of **1993** or the **26/11 terror strike** in Mumbai in 2008. With the existence of a number of critical facilities along the coastline like ports, oil refineries, etc. the vulnerability to security threats has increased many folds as these critical infrastructures are **high valued targets** for the terrorists. There is also the problem of rampant **piracy** across the western Indian Ocean and the Arabian sea. These pirates attack the ship coming from the routes like the Red Sea. These not only pose threat to the **financial assets** of the country but also jeopardize **national security** by attacking ships containing oil or natural gas reserves.

United Nations Convention on the Law of the Sea (UNCLOS), has defined "**Piracy**" as any illegal act of violence or detention committed for private ends by the crew or the passengers of a private ship against any other ship on the **high seas** (open sea that does not fall under the jurisdiction of any country). There have been incidents of Somalian piracy extending eastwards into and across the Lakshadweep. In 2012, the longitudinal marking for high-risk areas for piracy was moved by International Maritime Organization from the west of Lakshdweep at 65 degrees east to its east at to 78th meridian east.

The proneness of western Indian Ocean to piracy directly threaten India's interests on multiple fronts. India's maritime trade faces disruption from incidents of violence or risk of hostage situations. The shipping industry stands to lose due to requirement of higher insurance premiums. The cost of sea-based trade increases and the attractiveness of ports serving this trade declines. Given India's plans for port-led growth on its long coast, piracy is a concerning risk. Moreover, the reputation for the region of being unsafe can become excuse for outside interventions and naval presence of extra-regional powers. The Chinese military base in Djibouti or USA's presence in Diego Garcia are a case in point. Piracy can thus lead to militarization of high seas in India's vicinity, posing grave threat to India's national security and sovereignty.

Q. In 2012, the longitudinal marking for high-risk areas for piracy was moved from 65 degrees east to 78 degrees east in the Arabian Sea by the International Maritime Organisation. What impact does this have on India's maritime security concerns? **(UPSC 2014)**

There is rampant smuggling of **consumer and intermediate goods**, narcotics, arms, and gold, etc. through the sea routes. The smuggling of such goods is not only a threat to national security but also to national reserves. Smuggling of such contraband is often done by **terror organizations or their affiliates**, to further their anti-national activities. Further, smuggling has an intimate relationship with **money laundering**, as contraband smuggling is paid via money that is laundered by illegitimate activities and tax evasion, which is a grave threat to the country's economy. Large-scale refugee influxes over the last decades have resulted in widespread political turmoil in the border states. For example- The **creek areas of Gujarat** which have their geographical proximity to Pakistan and have complex terrain are conducive for infiltration. Political turmoil, religious and political persecution, overwhelming poverty, and lack of opportunities in Sri Lanka and Bangladesh provide the ground for the **illegal migration** of Bangladeshi and Sri Lankan citizens to India.

Often fishermen equipped with **poor technology** boat wander off from the Indian side to the waters of these countries. These fishermen are then caught for illegally trespassing into the sovereign territories of another country and are thus imprisoned. The issue is then further complicated by border disputes for example around the **Sir Creek region** between India-Pakistan and **Katchatheevu island** between India-Sri Lanka. However, there have been intelligence inputs that fishermen caught by Pakistan could be radicalized by Pakistani agencies like ISI to carry out terrorist attacks in India after returning. The fishermen issue further complicates **political friction** between India and these countries. Further, there is ever present risk of piracy on the high seas. Given the long coastline – 7516 kms, across 9 states and 4 UTs - coastal security and protection of maritime borders is a crucial aspect of border management for India. Coastal security is critical for maritime security.

Katchatheevu is an uninhabited island that India ceded to Sri Lanka in 1974 based on a conditional agreement called the "Kachchativu island pact". Later on, Sri Lanka declared Katchatheevu, a sacred land given the presence of a Catholic shrine. The central government recognizes Sri Lanka's sovereignty over the island as per the 1974 accord. But Tamil Nadu claimed that Katchatheevu falls under the Indian territory and Tamil fishermen have traditionally believed that it belongs to them and therefore want to preserve the right to fish there.

11.10.2.Issues Remaining in Coastal Security

One of the most notable issues is the **shortage of manpower** to guard India's seas. The marine police stations are not functioning effectively due to a **shortage of manpower and a lack of interceptor boats**. The then Defence Minister Nirmala Sitharaman informed the Lok Sabha in 2017 that the Navy faces a **20.68% shortage of sailors and 12.12% of naval officers**. It leads to the problem of inadequate patrolling. A cumulative shortfall (over 90 percent) in the patrolling efforts, especially at night, and a decline in physical checks on fishing vessels by the Coastal Police is a major security gap.

Though marine police are tasked with overall coastal security they are **not trained for counterterrorism**. Recently, the government has ordered the closure of an ambitious project to set up the country's first academy to train police forces in coastal security, because of financial constraints. The other significant issue is the **lack of a cooperative mechanism** between different security agencies. Many agencies like the Navy, Coast Guard, Marine Police, and other authorities are tasked with coastal security. The **absence of common infrastructure** creates a gap in carrying out various counter-terrorism operations. Also lack of coordination between the state-controlled marine police with central forces leads to poor sharing of important local intelligence as well as causes turf wars between the two. Further, extension of the jurisdiction of BSF, by the central government has been objected to by many state governments. Such issues could lead to poor coordination between BSF and state police.

11.10.3. Way Forward

Firstly**, there is a lacuna in the legislative and policy framework** with regard to coastal security. Comprehensive legislation must be enacted to place systems and processes for the protection of India's coast and its maritime infrastructure, covering both the shipping and port sectors. Further, the government must promulgate a **National Commercial Maritime Security Policy**, to clearly articulate its strategic vision for maritime security and to create deterrence.

Secondly, there is a need to **strengthen the Coast Guard and coastal police**, The CG must be strengthened by removing all ambiguities from the Coast Guard Act. There should be a clear **command chain and defined standard operating procedures** with reference to coastal security. State police agencies may be integrated into the **detection and capture of criminals** at sea, leveraging their unique access to fishermen and local communities, facilitating the flow of vital human intelligence. Further, there should be regular interagency **Security exercises**. Coastal security exercises like **Sagar Kavach** and **Sea Vigil** need to be conducted

regularly, in order to **generate awareness** about threats emanating from the sea as well as to develop synergies among the concerned agencies.

Lastly, the recently developed **IMAC (Information management and Analysis center)** is a also novel step in the right direction. IMAC is the nodal center for maritime security information collation and dissemination to security agencies for taking timely measures. It is being jointly operated by the **Navy and Coast Guard**. Currently, the IMAC only monitors **non-military or commercial shipping**, also known as **white shipping**. The IMAC monitors the movement of ships in the entire Indian Ocean region and reports to authorities, in case any suspicious activity is monitored. IMAC is not only able to share such data with domestic agencies but also share and collates data from other international security agencies. So, such technology incorporation should be promoted and other coastal nations should be included to enhance the data monitoring. As it is a well evident fact that we **cannot change our neighbors**, maintaining **friendly and cooperative relations** with the neighboring countries is not only an imperative for **regional peace** but also a pragmatic way to **protect and preserve** our borders.

Q1. Cross-Border movement of insurgents is only one of the several security challenges facing the policing of the border in North-East India. Examine the various challenges currently emanating across the In-dia-Myanmar border. Also, discuss the steps to counter the challenges. **(UPSC 2019)**

Q2. Border management is a complex task due to difficult terrain and hostile relations with some countries. Elucidate the challenges and strategies for effective border management. **(UPSC 2016)**

Q3. How far are India's internal security challenges linked with border management particularly in view of the long porous borders with most countries of South Asia and Myanmar? **(UPSC 2013)**

Various Security Forces and their Mandate

12.1. INTRODUCTION

India's territorial integrity and its security is maintained by Indian security forces which comprises of Indian Armed Forces, Paramilitary and Central Armed Police Force. The Indian armed forces comprise of Indian Army, Indian Navy, Indian Airforce, and Indian Coast Guard. They are mandated to both defend the country as well as launch an offensive on any adversary state.

12.2. INDIAN ARMED FORCES

12.2.1. Indian Army

Indian Army's primary role is to ensure the national security by safeguarding **sovereignty** and **territorial integrity** of the country from external aggressions and threats. It is also involved in providing **humanitarian aid** and assistance to civil authority during **calamities** and **natural disasters**. The Indian Army has approximately 14 lakhs active personnel in its ranks. The President of India is the Supreme Commander of the tri forces– Army, Navy and Air Force. The Army headquarters is situated in New Delhi and it is under the direction of the **Chief of the Army staff (Commander-in-Chief)**. He is a **four star General** and is assisted by a Vice Chief of Army Staff (VCOAS). Since independence, the Indian army has been involved in four wars with Pakistan (1947, 1965, 1971, 1999) and one with China (1962). Some other operations undertaken by the army include **Operation Vijay** (**Kargil War in 1999**), **Operation Meghdoot** (to gain control over Siachen Glacier in 1984) and **Operation Cactus** (to stop a Military Coup in Maldives in 1988). Despite operational and internal security commitments, the Indian Army is also involved in contributing to **United Nations Peacekeeping Missions** and is the second largest troops' contributor (**for 2021**) in various UN missions. Currently, four UN Peace Keeping contingents of India are deployed across the world.

> Field Marshal is a **five-star general officer rank**. It is the highest attainable rank in the Indian Army. It is a ceremonial or a wartime rank, having been awarded only twice in Independent India. The first Field Marshal of India was **Sam Manekshaw** who was conferred the rank on 1 January 1973, and the second, **K M. Cariappa** who was conferred the rank on 15 January 1986. As the Field Marshals never retire, the allottee holds the title for life.

12.2.2. Indian Navy

Indian Navy is a **well-balanced three-dimensional force** meaning that is capable of carrying out operations above, on and under the surface of the oceans, effectively to safeguard India's national interests. The Indian Navy works in conjunction with other Armed Forces of the country to deter or defeat any threats or aggression against the territory, people or maritime interests of India, both in times of war and peace. It also **projects India's influence** in country's maritime area of interest, to further the nation's political, economic and security objectives. It also works in close co-operation with the **Indian Coast Guard**, ensuring order and stability in India's maritime

zones of responsibility. Moreover, it also carries out **Humanitarian Assistance and Disaster Relief (HADR)** operations in times of natural disaster in **India's maritime neighborhood**.

The Indian Navy is headed by the **Chief of the Naval Staff (CNS), a four-star officer.** The Indian Navy's headquarter is located in New Delhi. The Indian Navy presently has approximately 69,000 active personnel. The Indian Navy is also considered as a **blue water Navy**.

According to the **Indian Maritime Doctrine, 2015** the ability to undertake distant operations across the globe without being required to reach back home for refueling is considered as **blue-water navy**. It states that distant operations rely upon the attributes of access, mobility, sustenance and reach in order to show presence, project power and/or accomplish other national objectives in the area of interest. As the Indian Navy has the potential to carry out distant operations "at or from the sea, up to considerable distance from national shore bases", it qualifies as a Blue Water Force.

12.2.3. Indian Air Force

The Indian Air Force (IAF) is the aerial arm of the Indian armed forces. It secures and protect the Indian airspace from any threat and conducts air warfare during a war. It is the youngest arm of the Indian Armed Forces. It was established by the British Empire in 1932, as an ancillary of the Royal (British) Air Force. The IAF currently has approximately 1.4 lakh active personnel. The Chief of the Air Staff, an air chief marshal, is a four-star officer, who is responsible for the bulk of operational command of the Air Force.

The rank of **Marshal of the Air Force** has been conferred by the President of India to **Arjan Singh** who became the first and the only five-star rank officer of the IAF so far. The IAF has also played an active role in HADR operations. It has provided assistance in relief operations during natural calamities such as the Gujarat cyclone in 1998, the tsunami in 2004, and Uttarakhand floods in 2013. The IAF has also undertaken relief missions to other countries such as **Operation Rainbow in Sri Lanka**.

12.2.4. Indian Coast Guard (ICG)

The Indian Coast Guard was established on the recommendations of KF Rustamji Committee (setup in 1974) on 18 August 1978 by the Coast Guard Act, 1978 of the Parliament of India. It operates under the aegis of **Ministry of Defence** and is headquartered in New Delhi. It protects the country's maritime interests and maritime law enforcement with jurisdiction over both territorial and international waters. This includes both the **contiguous zone and exclusive economic zone(EEZ)** ,i.e. it patrols the distance between the shore to 200 nautical miles. It is responsible for **marine environment protection** in maritime zones of India and is coordinating authority for response to oil spills in Indian waters. It works in close cooperation with the Indian Navy, Department of Revenue (Customs), Department of Fisheries, and the Central and State police forces.

Contiguous Zone and Exclusive Economic Zone

Contiguous Zone: As per the 1982 United Nations Convention on the Law of the Sea (**UNCLOS**), the contiguous zone is the water territory **extending up to 24 nautical miles** (i.e., 44 km) extending from the coastal baseline. The state and its agencies have a limited control over the contiguous zone for preventing and punishing offences like infringement of customs, immigration, sanitary laws and regulations and fiscal matters. In this zone the country can enforce laws only in four domains i.e., pollution, taxation, customs and immigration.

Exclusive Economic Zone: An Exclusive Economic Zone extends from the coastal baseline to up to 200 nautical miles (i.e., 370.4 km). The contiguous zone is also included in the EEZ. In this area, the country has sole exploitation rights over all the natural resources. In the EEZ of a country, the foreign vessels have freedom of navigation (FON) and

Border Road organization

BRO is a modern construction organization that is committed to meeting the **strategic requirements** of the Indian armed forces. The Border Roads Organization (BRO) functions under the control of the **Ministry of Defence**. This organization is responsible for constructing and maintaining the road networks in the border areas of India. It is also involved in developing road infrastructure in neighboring countries like Afghanistan, Bhutan, Myanmar etc. Its personnel are both drawn from **Indian Army** and also **directly recruited**.

12.3. CENTRAL ARMED POLICE FORCES (CAPFS)

The internal security of the country is looked after by Central Armed police forces comprising different forces with different mandates. Central Armed Police Forces were formerly known as Paramilitary Forces. However, from March 2011, the Ministry of Home Affairs (MHA) adopted a standard nomenclature of Central Armed Police Forces to avoid confusion. There are seven Central Armed Police Forces under the Union Government, namely- Border Security Force (BSF), Indo-Tibetan Border Police (ITBP), Central Reserve Police Force (CRPF), Central Industrial Security Force (CISF), Sashashtra Seema Bal (SSB), National Security Guard (NSG) and Assam Rifles (AR). All CAPFs are headed by a **Director General (DG) rank officer**. Since their inception all DGs of the CAPFs have been derived from the **Indian Police Service (IPS)**.

12.3.1. Border Security Force (BSF)

The Border Security Force (BSF) is the principal Border Guarding police force of India. It was raised in the wake of the India-Pak War of 1965 on 1st December 1965, "for ensuring the security of the Indian border and for matters connected therewith." Its operational responsibility is spread along the international border of Indo-Pakistan and Indo-Bangladesh which is over 7000 km. BSF is under the control of the Ministry of Home Affairs (MHA). BSF is also deployed on LoC (Line of control) in J&K under operational control of the Army. It is currently the world's largest border guarding force with over 2.5 lakh personnel to its name. BSF has been termed as the First line of Defense of the country. BSF is also the only Central Armed Police force to have its own Air Wing, Marine Wing and artillery regiments, which support the General-purpose Battalions in their operations. Three battalions from BSF are deputed to National Disaster Response Force (NDRF).

National Disaster response Force (NDRF) is world's first dedicated disaster response force. It was established in 2006 under the **Disaster Management act, 2005**. It functions under the control of **Ministry of Home Affairs (MHA)**. As of January 2022, there 16 battalions drawn from different paramilitary forces and deputed across various parts of the country.

12.3.2. Central Reserve Police Force (CRPF)

CRPF is the **largest force** among all the CAPFs. It was raised initially as **Crown Representative Police in 1939**. The Force was later rechristened as Central Reserve Police Force (CRPF) after Independence. It works under the control of the Ministry of Home Affairs (MHA). 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 law and order** and countering any subversive activities of militant groups. CRPF also has raised three NDRF Battalions to assist in relief operations during **natural calamities or any disasters**. It functions under the aegis of Ministry of Home Affairs (MHA) of the GoI. CRPF battalions are also stationed abroad as part of United Nations peacekeeping missions. Also, three battalions from CRPF are deputed to **National Disaster Response Force (NDRF)**.

Some specialized formations of CRPF are as follows:

The Rapid Action Force (RAF)

It is a specialized 10 battalion wing of CRPF. It was established in October 1992, with its headquarters in New Delhi to deal with riots and related civil unrest. It is a specialized force with multi-ethnic composition and better mobility for swift action to control communal riots. The personnel in RAF are trained and equipped to act as an effective Strike Force in riots or similar situations. These Battalions are located at 15 communally sensitive locations across the country to facilitate quick response in case of communal incidents.

Commando Battalions for Resolute Action (CoBRA)

The Government of India (GOI) had accorded approval for setting up CoBRA force for jungle/ guerrilla warfare operations to deal with insurgents, Naxalites and extremists etc.

The GOI accorded sanction of raising of 10 unattached battalions of CoBRA in CRPF and these battalions became operational during 2008-09. They are trained and equipped for commando operations especially against Left Wing Extremism (LWE) and are also capable of undertaking **intelligence operations**.

Special Duty Group (SDG)

SDG is raised as an elite CRPF unit, tasked to provide protection to the residence of the SPG protectee, for example, SDG is tasked with providing security for the **outer cordon of the PM's official residence**. It has personnel drawn from various units of CRPF. SDG members are also trained in handling nuclear and rescue operations, bio-chemical attacks, and behavioral management.

Parliament Duty Group (PDG)

PDG is also an elite CRPF unit tasked to provide protection to **Parliament House**. The idea of creation of the PDG was mooted in the aftermath of the **2001 Parliament terror attack**. It comprises personnel deputed from various units of CRPF. PDG personnel are also trained in combating nuclear and bio-chemical attacks, rescue operations and behavioral management.

12.3.3. Central Industrial Security Force (CISF)

Raised in the year 1969, CISF provides security cover to important and sensitive infrastructure/ PSUs like space and nuclear energy establishments, seaports, airports, steel, thermal and hydel power plants, oil and petrochemicals installations, heavy industries, defence establishments, security presses, museums, and historical monuments etc.

The specialized task of airport security was assigned to CISF in the wake of the hijacking of the Indian Airlines plane to Kandahar. 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 both public and private sectors. After the **26/11 Mumbai attack of 2008**, the mandate of the force was further broadened to provide **direct security cover to the private sector**. The Indian Parliament in 2009 authorized the CISF to provide security cover to private and cooperative establishments across the country for a certain fee by passing CISF (Amendment) Act, 2008. The Act further provides for deployment of CISF to **protect Indian missions abroad**. Like other CAPF's, CISF is also headed by an IPS officer and works under the aegis of Ministry of Home Affairs (MHA). Two battalions from CISF are deputed to **National Disaster Response Force (NDRF)**.

12.3.4. Indo-Tibetan Border Police (ITBP)

Indo-Tibetan Border Police Force was raised in the wake of the Sino-India war in 1962 and is headquartered in New Delhi. ITBP is headed by an IPS officer and is under the control of the Ministry of Home Affairs (MHA). ITBP is a mountain trained force called **"Himveer"** and most of the personnel are professionally trained mountaineers and skiers as it is deployed at an altitude of up to 21000 feet. Presently, majority of ITBP battalions are deployed

on the India-China border from Karakoram Pass in Ladakh to Diphu La in Arunachal Pradesh. ITBP plays a pivotal role in organizing the annual **Kailash Man Sarovar Yatra** besides assisting in disaster management and carrying out relief measures in the central and western Himalayan regions. ITBP is also at the forefront of the movement for the preservation of **Himalayan environment & ecology**. ITBP conducts a number of programmes in remote border and terrorist affected regions to provide free and expert medical interventions and hygiene care to the civilian population in those remote villages. Further, two battalions from ITBP are deputed to **National Disaster Response Force (NDRF)**.

12.3.5. Sashastra Seema Bal (SSB)

It was setup initially as **Special Service Bureau (SSB) in early 1963** in the wake of India China conflict of 1962 to boost people's morale and inculcate the spirit of resistance in the border population against threats of subversion, infiltration, and sabotage from across the border. Later, the Force was rechristened as Sashastra Seema Bal and its charter of duty was also amended and it came under the control of Ministry of Home Affairs (MHA). It has been given the responsibility to guard India's border along **Nepal and Bhutan**. It also serves as lead intelligence agency **(LIA)** for Indo-Nepal border and Indo-Bhutan border. It promotes a sense of security among the people living in the border area and **prevents trans-border crimes**, smuggling and other illegal activities and unauthorized entries into or exit from the territory of India. SSB is also being deployed in Jammu-Kashmir for counter-insurgency operations and anti-Naxal operations in Jharkhand and Bihar. It also performs internal security duties, like election duties and law and order enforcement duties, in different parts of India. Further, two battalions from SSB are deputed to **National Disaster Response Force (NDRF)**.

12.3.6. National Security Guards (NSG)

The **National Security Guard (NSG)** is a special force set up in 1986 as a Federal Contingency Deployment Force to carry out counter-terrorism activities. The idea was mooted in the **backdrop of Operation Blue Star, 1984**. It was created under the National Security Guard Act, 1986. It works completely within the Central Armed Police Forces structure. NSG is a **purely deputation force** and all personnel posted are on deputation from Army, CAPFs, State police and other organizations. Its primary task is to engage and neutralize terrorist threats in specific situations and undertake **counter hijack** and **hostage rescue** missions. They are also assigned the task of providing security protection to VVIPs. The NSG personnel are often referred to as **'Black Cats'** because of the black outfit and black cat insignia worn on their uniform. NSG is headed by an IPS Officer and is under the administrative control of the Ministry of Home Affairs (MHA). The NSG's specific goals include: neutralization of terrorist threats, handling hijack situations in air and on land, **Bomb disposal** (search, detection and neutralization of IEDs), engaging and neutralizing terrorists in specific situations and hostage rescue. NSG performed Operation **Black Tornado** and **Operation Cyclone** to flush out terrorists and rescue hostages after multiple attacks across Mumbai in the 26/11 attack in 2008. The **National Bomb Data Centre** (NBBC) under NSG maintains the National Bomb Data Centre at Manesar, Haryana and conducts **post blast studies** in various parts of the country mostly on request from State authorities. It maintains a data bank on explosives and incidents of blasts which may be of use to security forces.

12.3.7. Assam Rifles (AR)

Assam Rifles is known as 'Friends of the Hill People' and 'Sentinels of the North-east'. Assam Rifles was raised initially as **Cachar Levy** in 1835, and is the oldest police force in the country with headquarters at Shillong. Acknowledging their role in the first world war, the Britishers renamed it as Assam Rifles. The Force has a dual role of maintaining internal security in the North Eastern region and guarding the Indo-Myanmar Border.

Post-independence, their role has been evolving and they have performed many roles. This includes internal security, counter insurgency, border security operations, provision of aid and assistance to the civilians in times of emergency, and the

provision of communications, medical assistance and education in remote areas. During the 1962 Sino-Indian War Assam Rifles were used to delay the advancing Chinese forces so that the Indian Army could establish their defence lines across the border. Three battalions of Assam Rifles were deployed on **Operation Pawan** in Sri Lanka between December 1988 and February 1990. Recently, the Ministry of Home Affairs (MHA) proposed that the Assam Rifles should be merged with the Indo-Tibetan Border Police (ITBP). Currently, the Assam Rifles is under the administrative control of the **Ministry of Home Affairs** and **operational control of the Army**, i.e., the Ministry of Defence. This **duality of administrative** control and operational control leads to **problems of coordination**.

In their working the CAPFs face a number of challenges. Indian borders run through diverse terrain including **deserts, marshes, plains and mountains.** The **terrain, climate and porosity of borders** poses a challenge to forces in its effective management of the borders. Further, the deficit of critical infrastructure such as **roads, observation towers, bunkers, border flood etc.,** creates a plethora of operational difficulties for the troops. The CAPFs often lag behind in leveraging technology. Despite provisions like CIBMS, the security forces still lack **hi-tech equipment such as sensors, detectors, cameras, ground-based radar systems, etc.** and are **ill-equipped** to manage border issues given poor intelligence capabilities. Absence of a unified command and control is evident as **multiple forces are overseen by different organizations**. It leads to lack of coordination, poor intelligence and even conflicts. For instance, **SSB** guards the **Sikkim border with Nepal and Bhutan** and **Assam Rifles** guards the **Arunachal Pradesh, Nagaland, Manipur and Mizoram borders**. Further, coordination with the army and police force in Kashmir is another challenge. Although the CAPFs work in as challenging and difficult conditions as the Army there is a tangible **non-parity vis-à-vis the army** in terms of facilities and salaries. This not only demoralizes the troops but also keeps the best talent away from joining the CAPFs. Further, these forces are **headed by IPS** officers, who are seen as **outsiders** to the force, and there is no system for regular personnel of the CAPF to reach the top level and head these organizations. In addition to these issues there is the challenge of long working hours, **poor work life balance, low pay, poor training** etc. resulting in **clashes** between officers and men, **frustration** and even **suicide** in some extreme cases.

CAPFs are **an important apparatus** for upholding the country's security. They are vital for tackling internal security threats emanating from LWE, as they are instrumental in keeping a strict vigil along India's long international borders. In this light, it is important to effectively **resolve the challenges** faced by the CAPF personnel. In this light leveraging technological advancements on one hand can improve **the security paradigm** at the borders and at the same time **reduce the operational difficulties** of the troop. Drones, laser fence, CCTV camera, radar systems etc., should be used **to ease round the clock surveillance** through difficult border terrain. Since there are multiple CAPFs, smooth coordination between them is warranted for effective delivery of their mandate. For this **agreement on basic guiding principles and SOPs** is required among forces. Increasing **CBMs** (Comprehensive Border Management) and communication linkages are must to avoid unnecessary confrontation. Further **Infrastructure** along with border must be improved. **Rail connectivity** along with **road connectivity** must be provided for quick and timely mobilization of troops. Since all CAPFs work in physically and mentally challenging situations a better work life balance is a must. Focus on **mental and psychological health**, better **training** institutes and **pay parity** with the army have to be established. Last but not the least, there is a need for **grooming officers from entry level** so that suitable candidates for the top post can emerge from within the force.

12.4. OTHER PARAMILITARY FORCES

A paramilitary is basically a semi-militarized force whose organizational structure, training, culture, tactics, and often function are similar to those of a professional military, but they are not formally part of a country's armed forces. The term "paramilitary forces" in India has **not been defined**

in any act of Parliament or by the authorities. Since 2011, the Government of India (GoI) uses an unofficial definition that the Paramilitary forces are the ones that assist the military forces and are headed by Military officers, not by IPS officers.

12.4.1. Special Frontier Force (SFF)

It is based in **Uttarakhand**. SFF is the first special force of independent India and is also referred to as **Vikas Battalion**. Special Frontier Force or Establishment 22 was an outcome of the 1962 India–China War. Its main goal originally was to conduct covert operations beyond the Chinese lines in the event of another Sino-Indian War. In peacetime, they operate as a second line of defence in conjunction with the ITBP. This concealed special force operates under India's intelligence agency Research and Analysis Wing (RAW) and reports directly to the **Prime Minister** through the Directorate General of Security in the **Cabinet Secretariat.** On the ground, it is headed by an Inspector General who is an Army officer of the rank of Major General.

12.4.2. Special Protection Group (SPG)

The Special Protection Group (SPG) is the executive protection agency of the GoI. It is responsible for the protection of the Prime Minister of India, former Prime Ministers and their immediate family members. The Force is under the control of the Cabinet Secretariat. It was established in 1985 by SPG Act after the assassination of Mrs. Indira Gandhi, the then Prime Minister. After the assassination of Mr. Rajiv Gandhi, the act was amended to provide security cover to former prime ministers as well. SPG comprise of ring round teams, isolation cordons, the sterile zone around, and the rostrum and access control to the person or members of his immediate family. The Act was amended again in 2003 to bring the period of automatic protection from 10 years to "a period of one year from the date on which the former prime minister ceased to hold office" and thereafter based on the level of threat as decided by the government. The senior and junior officers of SPG are recruited from the Indian Police Service (IPS), Central Industrial Security Force (CISF), Border Security Force (BSF) and Central Reserve Police Force (CRPF). No single individual serves in SPG for more than one year. SPG personnel are sent back to their parent unit after completing their tenure.

SPG Act was **amended in 2019** to reduce SPG cover to only the Prime Minister and members of their immediate family residing with him at his official residence. The 2019 amendment further reduce the time period of SPG cover to the former Prime Ministers and their immediate family to five years after they leave the office, provided that the immediate family members resided at the allotted residence with the former Prime Minister.

The amendment act, 2019 states that when the proximate security is withdrawn from a former Prime Minister, such proximate security will also stand withdrawn from members of his immediate family.

12.4.3. Railway Protection Force (RPF)

The Railway Protection Force (RPF) of the Indian Railways is entrusted with the task of protecting the Indian Railways and its passengers. RPF was established by the **Railway Protection Force Act, 1957**. The force works under the authority of the **Ministry of Railways**. The present strength of RPF is approximately around 65,000. The duties of the RPF include, to engage in all conducive means for the free movement of the railways, protection and safeguarding of railway property and its passengers as well as their belongings. Initially, the force was called Watch & Ward and it functioned under the administrative control of railway administration. Later on, this force was renamed as Railway Protection Force (RPF) and its personnel were authorized to arrest without warrant for the unlawful possession or damage to railway property. It has also been given the power to search, investigate, arrest, and prosecute offences committed only under **Railway Property (Unlawful Possession) Act 1966, The Railways Act, 1989**. However, the power of arrests under other penal provisions lies in the hands of the Government Railway Police (GRP) of state police.

12.5. CENTRAL INTELLIGENCE AGENCIES

12.5.1. Intelligence Bureau (IB)

The Intelligence Bureau (IB) is India's premier internal intelligence agency. It was recast as the Central Intelligence Bureau (earlier called as **Indian Political Intelligence (IPI)**) in 1947 under the **Ministry of Home Affairs**. IB garners intelligence from within the country and also execute counter-intelligence and counter-terrorism measures. The Director IB (DIB), who is a member of the **Joint Intelligence Committee (JIC)**, is the chief of Intelligence Bureau. The Bureau comprises employees from various law enforcement agencies including Indian Police Service (IPS) and the military. It coordinates with various states' police all over the country.

12.5.2. Research and Analysis Wing (RAW)

Until 1968, the Intelligence Bureau (IB), was responsible both for India's internal intelligence as well as external intelligence. But after India's debacle in the 1962 border war with China, the need for a specialized external intelligence agency was felt. As a result, India established the Research and Analysis Wing (RAW) in 1968. It was founded mainly to focus on China and Pakistan, however over the last fifty years the organization has expanded its mandate and is credited with greatly increasing India's influence across the globe.

Experts say RAW's powers and its role in India's foreign policy have varied under different prime ministers. RAW has contributed to several foreign policy successes like the **creation of Bangladesh in 1971**, the accession of Sikkim in 1975, the security of **India's nuclear program**, the success of African liberation movements during the Cold War. In 2004, GoI added yet another technical intelligence agency called the National Technical Facilities Organization (NTFO), which was later renamed as **National Technical Research Organization (NTRO)** after encountering technical intelligence gaps in the build up to the Kargil war. The agency has expertise in technology intelligence capabilities in areas like aviation and remote sensing, data gathering and processing, cryptology systems, strategic hardware, cyber security and software development and strategic monitoring.

National Technical Research Organization (**NTRO**) was set up as a technical intelligence agency in 2004 under the National Security Advisor in the Prime Minister's office. The Group of Ministers (GOM) headed by then Deputy Prime Minister L K Advani has recommended the constitution of a state-of-the-art technical wing of intelligence gathering. It follows the same "norms and conduct" as the Intelligence Bureau and Research and Analysis Wing. It serves as the super-feeder agency for providing technical intelligence to other agencies on matters of internal and external security.

12.5.3. Narcotics Control Bureau (NCB)

The Narcotics Control Bureau was created in 1986 to enable the full implementation of the **Narcotic Drugs and Psychotropic Substances Act, 1985** and fight its violation through the Prevention of Illicit Trafficking in **Narcotic Drugs and Psychotropic Substances Act, 1988**. NCB coordinates between the union and state authorities for ensuring compliance of India's international obligations with regard to drug trafficking under various conventions, such as Single Convention on Narcotic Drugs (1961), the Convention on Psychotropic Substances (1971), and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances **(1988)**. NCB is the nodal drug law enforcement and intelligence agency of India responsible for fighting drug trafficking and the abuse of illegal substances. It works under the aegis of **Ministry of Home affairs (MHA)**.

12.6. CENTRAL INVESTIGATIVE AGENCIES

12.6.1. Central Bureau of Investigation (CBI)

The CBI is India's premier investigating agency. It traces its origin to the **Special Police Establishment (SPE)** of 1941. The functions of the SPE were to investigate cases of bribery and corruption in the backdrop of transactions during World War II. Later, the **Santhanam Committee report of 1964** on Prevention of Corruption recommended the establishment of the CBI. The CBI was then formed by a resolution of the Ministry of Home

Affairs. SPE was renamed as Central Bureau of Investigation on 1st April, 1963 and it draws its power from **Delhi Special Police Establishment Act,** 1946. However, CBI is a **non-statutory** body and this Act transferred the superintendence of the SPE to the Home Department and its functions were enlarged to cover all departments of Govt. of India. The control of CBI was later transferred to **Ministry of Personnel** and now CBI plays the role of an attached office under it. The jurisdiction of the CBI extended to all the Union Territories and could be extended also to the States with the consent of the State Government concerned. The superintendence of CBI related to the investigation of offenses under the Prevention of Corruption Act, 1988 lies with the Central Vigilance Commission (CVC) and in other matters with the Department of Personnel & Training (DoPT) in the Ministry of Personnel, Pension & Grievances of the GoI. The CBI is India's nodal agency for correspondence with the INTERPOL. Lokpal exercises power of superintendence and direction over the CBI in cases where the investigation has been referred to the CBI by the Lokpal.

12.6.2. National Investigation Agency (NIA)

NIA was created after the 2008 Mumbai terror attacks as the need for a central dedicated agency to investigate terror cases was realized. NIA acts as the central Counter-Terrorism law enforcement agency. The agency is authorized to deal with terror-related crimes across all states without any permission from the states unlike CBI which requires consent of state to investigate cases. However, NIA can investigate only certain cases which are given under the schedule of the Act that include offences under the Atomic Energy Act, Anti-Hijacking Act, SAARC Convention (Suppression of Terrorism) Act, Suppression of Unlawful Acts Against Safety of Maritime Navigation and Fixed Platforms on Continental Shelf Act, Suppression of Unlawful Acts against Safety of Civil Aviation Act, and Unlawful Activities Prevention Act (UAPA), 1967. The amendment in the NIA act, 2019 allows the NIA to investigate offences related to counterfeit currency or banknotes, human trafficking, manufacture or sale of prohibited arms, cyber-terrorism, and under the Explosive Substances Act, 1908. Under the NIA act, special courts have been notified by the GoI for the trial of the offences listed under the Act. The NIA Special Courts are empowered with all the powers of the court of sessions under Code of Criminal Procedure, 1973 for the trial of any offence.

Jurisdiction of the Central Bureau of Investigation (CBI)

DSPE Act, 1946 provides for CBI to act within the jurisdiction of any state, with the mandatory consent of the concerned state. Police is a state subject under List II, i.e., it is exclusively a state subject which sometimes leads to the problem of **overlapping jurisdiction**. A general consent is provided by the state governments to ensure seamless investigation in cases of corruption involving the central government employees working in the concerned state.

However, in recent times the CBI has been criticized for being a **political tool** especially in cases of states ruled by opposition parties. The bitter political fight has led to many states, such as Maharashtra, West Bengal, Punjab, Rajasthan etc., to withdraw their general consent. This has **hampered investigation** in various cases of national significance. For example, CBI has submitted before the Supreme Court that since 2018, there are at least 150 requests for consents pending before the states that have withdrawn the general consent for CBI investigations.

The issue of overlapping jurisdiction has reached before the Supreme Court and the central government has claimed that the power of the states to **withhold the consent** to the CBI is **not absolute**. As per the affidavit of the union government, CBI has power to register FIRs and investigate the cases related to entries in the list 1 (union list) of the schedule 7 and the withdrawal of consent will have no bearing in such cases. The Union government is of the opinion that certain cases may be **politically sensitive** and under the pressure of state government the state police cannot ensure a free and fair investigation. Depriving CBI jurisdiction in such cases will create a **legal vacuum** and deny justice to the aggrieved parties. Further, the Supreme court and the High Courts can order CBI to investigate any corruption crime anywhere in the country without the consent of the state.

Q. The jurisdiction of the Central Bureau of Investigation (CBI) regarding lodging an FIR and conducting probe within a particular state is being questioned by various states. However, the power of states to withhold consent to the CBI is not absolute. Explain with special reference to the federal character of India. (UPSC 2021)

12.7. Other Organisations in News

12.7.1. National Security Advisor (NSA)

The post of NSA was created in 1998 during the tenure of PM Atal Bihari Vajpayee and has become increasingly influential and powerful over the years with the rise of India on the world stage. The NSA acts as the secretary of the National Security Council (NSC) of India, and the chief adviser to the Prime Minister of India on national and international security policy, and oversees strategic and sensitive issues. The present NSA, Mr. Ajit Doval assumed office in May, 2014 and continues to hold office as on Jan, 2022. In December 1998, on the recommendations of the special task force headed by K.C. Pant, a three-tier structure was set up, consisting of:

1. The National Security Council (NSC)
2. Strategic Policy Group (SPG) and
3. National Security Advisory Board (NSAB).

The National Security Council of India is a three-tier organization that oversees political, energy, economic, and security issues of strategic concern to the country. Prime Minister is the ex-officio chairman of NSC and NSA acts as its secretary. It also consists of important members of the union cabinet directly concerned with national security issues like Home Affairs minister, Defence minister, Minister of Finance, Minister of External Affairs etc.

The Strategic Policy Group, which is chaired by NSA, consists of senior officials currently serving and responsible for policy-making and follow-up action in matters of national security. It includes the chiefs of the tri-services, i.e., Army, Navy and Air Force and also the chiefs of Intelligence Bureau (IB) and Research and Analysis Wing (RAW). Its main task is to make policy recommendations to the NSC.

The first **National Security Advisory Board** was set up in 1998. Its principal objective is to undertake long-term analysis and provide perspectives on issues of national security. The policy recommendations proposed by the NSAB are presented to the National Security Council for its consideration.

12.7.2. National Intelligence Grid (NATGRID)

NATGRID was first proposed in the aftermath of the terrorist attacks on Mumbai in 2008. NATGRID is an intelligence-sharing platform that collates data from the standalone databases of the various agencies and ministries of the Indian government. It is a counter-terrorism measure that collects and collates a host of information from 21 different government and private organizations that can be readily accessed by security agencies round the clock including tax and bank account details, credit card transactions, visa and immigration records and itineraries of rail and air travel. This combined data will be made available to 10 central agencies, which include: Research and Analysis Wing (RAW), the Intelligence Bureau (IB), Central Bureau of Investigation (CBI), Financial intelligence unit (FIU), Central Board of Direct Taxes (CBDT), Narcotics Control Bureau (NCB), Central Board of Excise and Customs (CBEC), Directorate of Revenue Intelligence (DRI), Enforcement Directorate (ED), and the Directorate General of Central Excise Intelligence (DGCEI). Initially, no state agencies will be given direct access to NATGRID data but in case any relevant information is required, they can approach NATGRID through any of 10 user agencies. The Data from NATGRID will help security agencies to identify any unscrupulous element and take preventive measures.

12.7.3. National Crime Records Bureau (NCRB)

The NCRB is an Indian government agency responsible for **collecting and analyzing crime data** as defined by the Indian Penal Code (IPC). NCRB is headquartered in New Delhi and functions under the Ministry of Home Affairs

(MHA), GoI. It was set-up in 1986 to function as a **repository of information** on crime and criminals so as to assist the investigators in linking crime to the perpetrators.

Crime and Criminal Tracking Network and Systems (CCTNS) is a project initiated in June 2009 by NCRB. It aims at creating a **comprehensive and integrated system** for enhancing the efficiency and effectiveness of policing at the Police Station level. It is an IT based state-of-the-art tracking system built for "investigation of crime and detection of criminals". CCTNS was envisaged as a **Mission Mode Project (MMP)** under the **National e-Governance Plan** of GoI. The system will digitize FIR, chargesheet data across all police station of the country. It will help in swift detection of criminals across the country and also reduce the delay in justice delivery system of the country.

Enforcement Directorate (ED): The directorate of Enforcement is a specialized financial investigating agency under the Department of Revenue, Ministry of Finance. It is entrusted by the Government of India, to enforce Foreign Exchange Management Act, 1999 (FEMA) and Prevention of Money Laundering Act, 2002 (PMLA), to effectively deal with various economic crimes. Economic crimes like illegal acquisition of foreign currency, malpractices regarding remittances of funds, siphoning off funds etc., come under the purview of ED.

Home Guard

'Home Guards' is a voluntary force, first raised in December 1946, to assist the police in controlling civil disturbance and communal riots. Subsequently, the concept of voluntary citizen's force was adopted by several states. In the wake of Chinese aggression in 1962, the Centre advised the states and Union

The role of Home Guards is to serve as an auxiliary Force to the police in maintenance of internal security situations, help the community in any kind of emergency such as an air-raid, fire, cyclone, earthquake, epidemic etc. The total strength of Home Guards in the country is 5,73,793.

12.8. CHALLENGES FACED BY BORDER SECURITY FORCES

There are few inherent challenges faced by the Border security forces of India but challenges of geographic terrain are most frequent and pervasive. Indian borders run through diverse terrain including **deserts, marshes, plains and mountains.** The **terrain, climate** and **porosity of borders** poses a challenge to forces in its effective management of the borders. The other challenge is lack of infrastructure in border areas. Critical infrastructure such as **roads, observation towers, bunkers, border flood lights etc.** are lacking. Security forces lack **hi-tech equipment such as sensors, detectors, cameras, ground-based radar systems, etc.** and are **ill-equipped** to handle border management given poor intelligence capabilities.

The deployment of **multiple forces is overseen by different organizations** leading to lack of effective coordination, poor intelligence and even conflicts. For instance, **SSB** guards the **Sikkim border with Nepal and Bhutan** and **Assam Rifles** guards the **Arunachal Pradesh, Nagaland, Manipur and Mizoram borders**. Further, coordination with the army and police force in Kashmir is another challenge. The other major challenge faced by security forces is issue of **non-parity with the Army** in terms of facilities and salaries which discourages forces. Further, these forces are **headed by IPS** officers, who are seen as **outsiders** to the force, and there is no system for regular personnel of the CAPF to reach the top level. Along with this, long working hours, **poor work-life balance, low pay, poor training** etc. results in **clashes** between officers and men, **frustration** and even **suicide** in some extreme cases.

Measures to be Taken

Technology upgradation and **use of technology** (drones, laser fence, CCTV camera, radar systems etc.) **to ease round the clock surveillance** through difficult border terrain. Government should take initiative to modernize weapon. An **agreement on basic guiding principles and common SOPs** is required among forces. Increasing **CBMs** (Comprehensive Border Management) and communication linkages are must to avoid unnecessary confrontation and escalation is

needed. **Infrastructure** along with border must be improved. **Rail connectivity** along with **road connectivity** must be provided for quick mobilization. Better work life balance, focus on **mental and psychological health,** better **training** institutes and **pay parity** with the Armed forces must be taken up as important tasks. Officers can be groomed **from entry level** so that suitable candidates for the top post can emerge from within the force. Keeping a strong vigilance on borders is important for any nation's security. To achieve synergy in efforts and operation of different border guarding forces the idea of **unified border protection force** can be explored.

Q. Analyze internal security threats and transborder crimes along Myanmar, Bangladesh and Pakistan borders including Line of Control (LoC). Also discuss the role played by various security forces in this regard. **(UPSC 2020)**

Defence Reforms

13.1. INTRODUCTION

The Indian defence forces are responsible for **protecting the country's sovereignty and integrity.** However, the rising security challenges from all across the globe, and particularly in the Indian backyard i.e., South Asia is a cause of concern. Further, the security **threats have been modernizing more rapidly** than the Indian defence forces, as the security threats evolve from conventional to non-conventional threats (like drone strikes, proxy wars, cyber-attacks, etc.). There is a **need to reform and modernize** our defence strategy to equip our forces to effectively and efficiently counter the evolving security threats and remove the already existing bottlenecks in the smooth functioning of our defence forces.

13.1.1. Historical Background

The **Kargil war of 1999** between India and Pakistan brought out the immediate need for reform in the Indian armed forces. The then government of **PM Atal Bihari Vajpayee**, set up the **Kargil Review Committee** to assess India's response to the war and suggest further reforms to streamline Indian Defence Forces. The committee analyzed the delay of Indian forces to respond to the Kargil intrusion and synchronism issue between the forces which led to a delay in aerial support to the Indian military by the Indian Air force. The committee then suggested several reforms like the setting up of a full-time **NSA (National Security Advisor), Chief of Defence Staff (CDS),** setting up of **Theatre commands,** etc. These recommendations were later reiterated by subsequent committees like the Standing **Committee on Defence in 2007**, the **Naresh Chandra task force in 2011, Ravindra Gupta task force in 2012**, and the **Shekatkar Committee in 2015**.

13.2. CHIEF OF DEFENSE STAFF (CDS)

Although the need for a CDS was articulated by several defense review committees, it was formally recommended by the Shekatkar committee report. Then, in 2019, the post of CDS was formally approved by **Cabinet Committee on Security (CCS)**. The CDS is a **four-star officer** just like other chiefs of Tri-services (Army, Navy, Air force). The CDS will be acting as the **single-point military advisor to the Defence Minister** on all Tri-services matters. The tenure of CDS is not fixed but an upper age limit of 65 years has been fixed. The Chief of Defence Staff will be acting as a secretary for the newly created **Department of Military Affairs (DMA)**, which would come under the aegis of the **Ministry of Defence (MoD).** The MDA would have members from both civil and military backgrounds. The CDS will also function as the Military Advisor to the **Nuclear Command Authority**. The CDS will also serve as the permanent chairman of the **Chief of Staff Committee**. However, it is important to note that CDS won't be commanding the three services chiefs.

The primary objective of the CDS is to: (i) bring about jointness in operation, logistics, training, support services, transport, communications,

repairs, and maintenance, etc. of the three services. (ii) ensure optimal utilization of resources and infrastructure by bringing jointness among the services. (iii) bring about reforms in the working of the three services with the aim to augment combat capabilities of the Armed Forces and reduce wasteful expenditure.

Nuclear Command Authority (NCA)

NCA is the authority responsible for command, control, and operational decisions with respect to **India's nuclear weapons program**. It has an Executive Council and a Political Council. The NCA's directives are executed by the **Strategic Forces Command**. The Executive Council is chaired by the **National Security Adviser (NSA)**. It gives inputs to the **Political Council**, which then authorizes a nuclear attack if the need ever arises. The Political Council is chaired by the **Prime Minister** and he is advised by the Executive Council.

The **Strategic Forces Command** is responsible for the management and operation of India's nuclear stockpile.

13.3. THEATRE COMMAND

A command is the highest organizational structure in the Indian armed forces. Each command is headed by **a Lieutenant General or a 3-star officer of the tri-services**. Currently, there are **19 military commands** of which 17 are service-oriented command, i.e. each service have their different sets of command: Indian army has 7 commands, Indian air force have 7 commands and Indian navy have 3 commands. Further, none of these commands are co-located and their geographical zones of responsibilities have little commonality, leading to lack of coordination in intelligence sharing , planning and execution. Thus, this military decentralization creates fault lines and impacts the effectiveness of Indian armed forces which was witnessed in the Kargil war, 1999. To overcome these issues, the various defense reform committees have suggested a **Theatre command**.

A theatre command is a broad military concept that addresses the multiplicity and complexity of modern warfare. The concept of theatre commands basically implies centralization of planning and execution of operations by allocation of resources under a single commander as against present cooperative planning and decentralized execution. So, **Theatre command is an integrated command** where the Tri-services work in unison in a warfare mode under a single commander (from any of the three services) for a given geographical area. The commander of the theatre command will not be answerable to individual services and will have the freedom to equip, train and exercise his command to make it a cohesive fighting force capable of carrying out both defensive and offensive roles. The commander will also bear all resources at his disposal, from the Army, the Navy, and the Indian Air Force.

Currently, India has **one theatre command operational at Andaman and Nicobar Island**. However, now in a bid to reform military organization, make Indian armed forces agile, and equip them to counter rising threats, the CDS of India is tasked with the establishment of theatre Command.

13.3.1. Advantages

Integrated Theatre Command will eliminate duplication of resources. For example, the Indian Army and Indian Air force both place orders for the same Apache attack helicopter separately, but with an integrated theatre command such resources can be shared between the forces, and thus the budgetary cost can be rationalized. Also, since the tri-services work together in a warfare mode, the forces get acclimatized to the operating procedure of the sister forces. This will enable them to communicate seamlessly and work effectively with each other in case of any exigency.

Since a theatre command is under the control of a single commander, his orders cut down the response time in any adverse situation, and help to exploit fleeting windows of opportunity in such situations. Further, joint forces provide the commander with multidimensional capabilities (land, sea, and air), that are more effective than single service forces, by providing a wider range of operational and tactical options. Additionally, multi-service capabilities allow a commander to combine capabilities of the services in asymmetrical as well as symmetrical ways to produce a total

military impact that is much greater than the sum of its parts. Lastly, across the world, major powers have recognized the importance of having an integrated military structure and countries like the USA, Britain, France, China, etc. have implemented an integrated armed forces setup.

13.3.2. Challenges

It has often been argued that for a benign power like India, whose primary objective is to safeguard territorial integrity, there is no need for the integrated theatre command. Moreover, Unified commands are essentially required for countries with global aspirations of carrying out missions across the world.

Another major challenge in the way of integration of the forces is the **inter-service rivalry**. As it is believed that the integration of forces will lead to loss of commanding authority and interference in their domain by the sister services. Thus, the top brass of these services, especially the Air force, are not very enthusiastic about Theatre command and tend to resist any change in the traditional hierarchy of these services.

Further, the country faces a **dearth of air resources**, which demands that air resources should be kept under centralized control (Indian Airforce). Also, air resources possess strategic mobility and can be easily moved from one command to another as per requirement. Thus, the paucity of air resources hinders the creation of theatre command.

Also, effective utilization of tri-service resources would **require specialized commanders** who have in-depth knowledge of the tri-services. However, currently, the officers are trained/spend their career in one service. Thus, there is a need to allow officers to work under different services to allow them to gain expertise about all services and only such individuals should be allowed to lead a theatre command.

13.4. SECURITY DOCTRINE

National security is the concept of securing the territory, citizens, and the interests of a nation. National Security is the responsibility of the government of that nation. In India, the Union government is responsible for National Security. It falls under **Union List** in the **seventh schedule** of the constitution.

Governments across the world, come out with a **national security doctrine**, which is a set of stated principles of government policy in different aspects of national security, like war, terrorist attack, armed insurgency, economic or political interference in national affairs, etc. The National security doctrine guides the political leaders by laying out countries' interests/priorities and threats to the country's interests. Further, it also helps to guide the government to deal with various exigencies. However, India presently does not have a national security doctrine.

13.4.1 Need for National Security Doctrine

Given India's history and geography, India faces a continuous threat from external as well as internal sources. Also, the nature of these threats has evolved with time but with no national security doctrine in place, India's response to such threats is ad-hoc and based on political preference. Thus, the Indian response changes to security threats every now and then. For example: During the Pathankot attack of 2016, NSG was deployed despite the Air force having its commando unit **"GARUD"** and army unit stationed nearby. India's responses towards such incidents have mostly been defensive and not offensive. Such responses create unease and uncertainty not only among the citizens but also the defense forces of the country.

Further, a well-defined National Security doctrine acts as a **deterrence against any uncalled adventurism by a state or non-state actor**. A clearly articulated response to a particular type of threat will deter any adversary from making any aggression towards the country and its citizens and their interests. Thus, would save the country from any harm. Also, after a national security incident, for e.g., a terror attack, different security and intelligence agencies start blaming each other and no one agency is held accountable because of a lack of understanding of the specific area of responsibility of various agencies.

Moreover, a national security doctrine will have a **standard operating procedure (SOPs)** based on specific threats. This will cut down any delay in responding to such threats. Further, a National

Security Doctrine will also act like a **'foreign policy tool'** and guide India's international relations towards adversary nations like Pakistan and also with our allies like Nepal, Bhutan, etc.

Lastly, India seeks to have a permanent seat in UNSC (United Nations Security Council) and project itself as a **'net security provider'** in the South Asian region. Thus, it is imperative for India to have a well-defined national security doctrine, to be a regional leader and a reliable partner.

National Security Doctrine in the US

In the US, every President assuming charge of the oval office is obligated under the law to bring and disclose a National Security Doctrine to the public, that he and his administration is going to follow. For example, **Donald Trump** on assuming charge of the President in 2017, made his National Security Strategy public, in which he mentioned that **America will no longer tolerate chronic trade abuses and will pursue reciprocal economic relationships**. According to the strategy, Donald Trump started what was famously called a **Trade war** with China. Further, the strategy also mentioned that **America would target threats at their source,** and in response to the statement, the US launched a drone strike to kill **Iranian commander Qasem Soleimani** whom the US perceived as a security threat to itself.

In comparison, India has no national security doctrine and its impact could be seen in case of a clash with China at **Galwan valley** in 2020 which led to the death of 20 Indian soldiers. India did not respond to the clash immediately, later it responded by banning over 118 Chinese apps operating in India. Thus, India's response was not only asymmetrical but untimely. Again, in the case of the Pulwama Terror attack in 2019, India responded by conducting an airstrike against terrorist hideout across the LoC in Pakistan. However, despite repeated ceasefire violations by Pakistan along LoC, India has not taken any credible steps from stopping Pakistan from doing so. Thus, an absence of national security doctrine makes India's response to security threats highly variable and often asymmetric.

13.5. RECENT REFORMS IN THE DEFENCE SECTOR

As **Stockholm International Peace Research Institute (SIPRI)** reports India has been the 2nd largest arms importer for the period 2016-20. Such heavy reliance on foreign imports to fulfill security needs creates critical vulnerability in national defense. To address these vulnerabilities, the government had brought several reforms in the defense sector, under its **Atmanirbhar Abhiyan (Self-Reliance campaign)**.

The defense sector is extensively promoted under the **Make in India** campaign. In August 2020, the import of several non-critical defense equipments was stopped. Further, to boost investment in domestic production in India's defense sector, the **FDI limit (Foreign Direct Investment)** has been increased from the earlier **49%** to **74% through automatic route** and **beyond 74% was permitted through government (approval) route**. With this impetus in domestic defense manufacturing, India not only aims to become self-sustainable in its defense requirement but also has vision to become a net defence exporter. India intends to become a global manufacturing hub for defence equipment.

The government has also made the decision to corporatize the **Ordnance Factory Board (OFB)**. The government has divided into 7 companies under 100% government-owned PSU, under the **Companies Act, 2013**. The Ordnance Factory board regulates several ordnance factories working under the **Ministry of Defence (MoD)**, these factories are responsible for fulfilling arms and ammunition requirements for Indian defence forces. The OFB continued to suffer from operational inefficiencies, as cited by **CAG (Comptroller and Auditor General)** report. The CAG also reported that in the year 2017-18, OFB was only to meet 49% of its expected demand. Since Indian armed forces remain heavily dependent on OFB for arms and ammunition, it was affecting the defense forces operational preparedness. Thus, on the recommendation of several committees like **TKA Nair Committee 2000, Vijay Kelkar committee 2005**, and **Raman Puri committee, 2015** the government in a bid to enhance the operational efficiency of this ordnance factory decided for the corporatization of OFB, including a public listing of

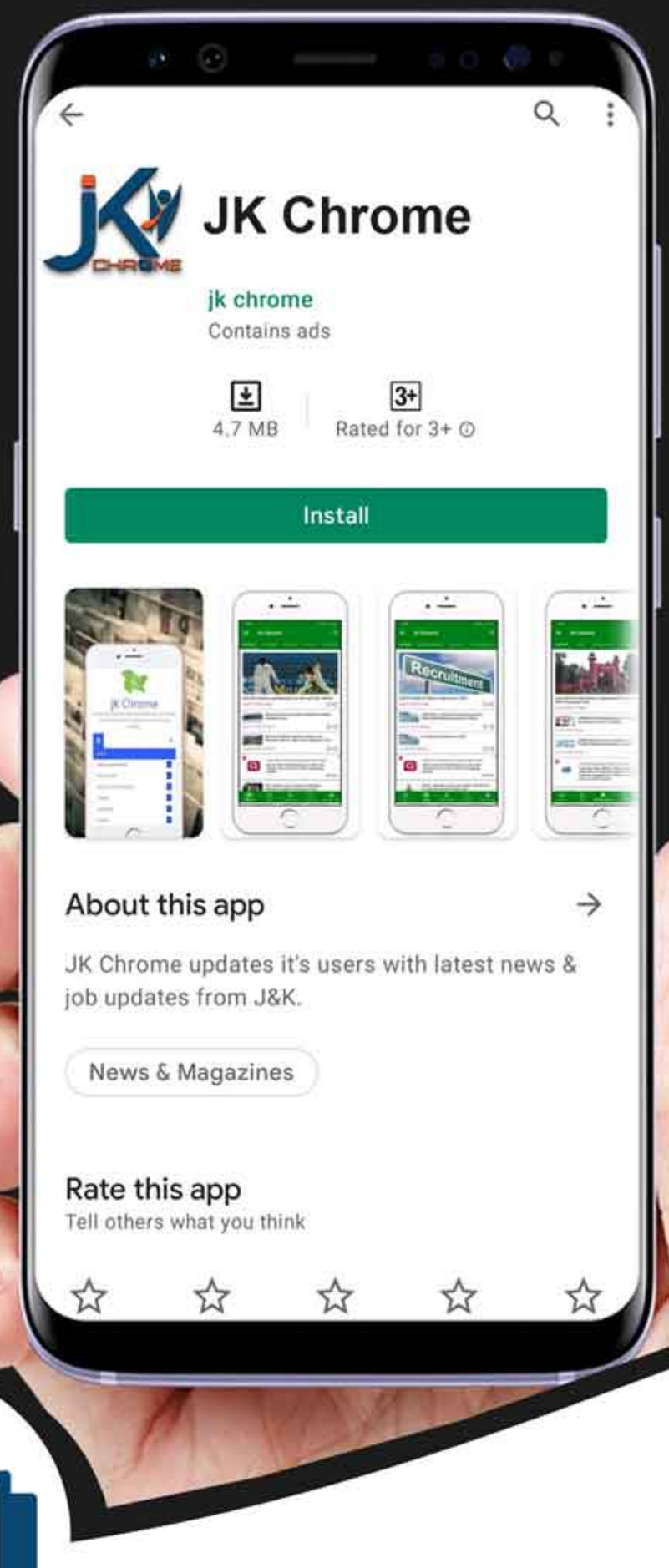
some units, thus ensuring a more efficient interface of the manufacturer with the designer and end-user.

The government has also come with the new **Defense Acquisition Procedure (DAP 2020)** for promoting indigenous design and development in defense & aerospace. The DAP has been designed to give preference to the domestic purchase of defense equipment. Additionally, the government has also earmarked a certain part of the budget for **domestic defence capital acquisition** to give impetus to the nascent domestic defence manufacturing industries.

■■■

JK Chrome

JK Chrome | Employment Portal



Rated No.1 Job Application of India

Sarkari Naukri
Private Jobs
Employment News
Study Material
Notifications

JOBS

NOTIFICATIONS

G.K

STUDY MATERIAL

GET IT ON Google play

JK Chrome
jk chrome
Contains ads

Click here to DOWNLOAD

www.jkchrome.com | Email : contact@jkchrome.com